Gruppo di lavoro dei General Counsel

Privacy e Data Protection: gestione dei dati in azienda alla luce delle nuove normative

Il Tavolo di lavoro “Privacy” si è riunito per esaminare il Regolamento (UE) 2016/679 – c.d. GDPR. Nel corso del lavoro comune, i partecipanti hanno analizzato l’evoluzione della normativa applicativa conseguente all’entrata in vigore del menzionato Regolamento, in un fattivo confronto tra operatori del diritto.

Il lavoro è stato condotto da cinque sottogruppi, che si sono impegnati nell’approfondimento teorico delle seguenti tematiche:

- **Condizioni di liceità del trattamento;**
- **Diritti degli Interessati**
- **Titolare e Responsabile del trattamento;**
- **DPO - *Data Protection Officer*;**
- **Trasferimento dei dati personali all’estero;**
- **Violazione dei dati.**

Sono stati altresì condivisi – ove possibile - casi concreti e valutazioni di eminente taglio pratico.

Il presente scritto costituisce un’occasione di riflessione che ci si augura sia di utilità anche a chi non ha partecipato al tavolo, così come lo è stato per i legali coinvolti, senza alcuna pretesa di esaustività su di un tema attuale, centrale e ancora in forte evoluzione.

Il documento è il risultato dell'attività svolta dal Gruppo di Lavoro guidato dall'Avv. Valérie Ruotolo, Head of Legal Dept. HP Italy S.r.l. e costituito da (in ordine alfabetico):

Andreoletti Michela Anna	HP Italy S.r.l.
Antonucci Paolo	Bolton Group
Baccetti Enrico Carlo	Boehringer Ingelheim Italia S.p.A.
Battista Andrea	Gruppo San Donato
Child Alexandre	Ecospray Technologies S.r.l.
Culot Elena	Tesi Elettronica e Sistemi Informativi S.p.A.
Cutolo Cristina	Consorzio Cepav Due
Di Salvia Elena	Milano Serravalle, Milano Tangenziali S.p.A.
Fierro Mariangela	Accenture S.p.A.
Formoso Francesca	ISS Facility Services S.r.l.
Frugiuele Giovanni	Accenture S.p.A.
Guagliardo Giorgio	Sguinzi Pietro S.p.A.
Marra Antonella	Universal Music Italia S.r.l.
Mauri Brunella	Agrati S.p.A.
Monti Alessandro	Banca Mediolanum S.p.A.
Morrone Marta	Accorhotels Italia S.r.l.
Pasquariello Silvia	Universal Music Italia S.r.l.
Piani Sonia	General Motors Italia S.r.l.
Poggiani Giorgio	Vision S.r.l.
Rapetti Paolo	Gruppo Cimbali S.p.A.
Restelli Antonio	Icap -Sira Chemicals and Polymers S.p.A.
Rinaldi Stefano	Gruppo Rentokil – Initial Italia S.p.A.
Scherillo Anna	Accenture S.p.A.
Tettamanti Gabriele	Gruppo San Donato
Tigani Federica	Hearst Magazines Italia S.p.A.
Tosetti Dardanelli Giorgio	Diners Club Italia S.r.l.
Vailati Elisabetta	Saipem S.p.A.
Vesurga Alessandro	Canali S.p.A
Vizilio Marta	Rentokil – Initial Italia S.p.A.
Zighetti Michela	Candy Hoover Group S.r.l.

1. CONDIZIONI DI LICEITA' DEL TRATTAMENTO

1.1 INFORMATIVA PRIVACY PER I DIPENDENTI

Egr. Sig. _____

INFORMATIVA RESA ALL'INTERESSATO PER IL TRATTAMENTO DI DATI PERSONALI COMUNI E PARTICOLARI AI SENSI DELL' ART. 13 del REGOLAMENTO UE 2016/679

La società XXX con sede legale in XXX, nella persona del suo legale rappresentante pro tempore XXX, in qualità di Titolare del trattamento, La informa - ai sensi dell'art. 13 del Regolamento UE 679/16 ("Regolamento")- di quanto segue:

1) **Finalità e base giuridica del trattamento**: I dati anagrafici e fiscali Suoi e dei Suoi familiari a carico, o comunque componenti del Suo nucleo familiare, e gli estremi del Suo conto corrente bancario, da Lei comunicati sono necessari per l'esecuzione del rapporto di lavoro, in particolare per l'elaborazione ed il pagamento della retribuzione e per ogni adempimento di legge e di contratto, ivi compresi quelli derivanti dalla contrattazione collettiva, anche nei confronti degli Istituti di previdenza e assistenza (obbligatorie ed integrative) e dell'Amministrazione Finanziaria. Il mancato conferimento dei dati personali di cui al precedente paragrafo impedirebbe l'instaurazione o la corretta prosecuzione del rapporto di lavoro. Questi dati personali sono, infatti, necessari per provvedere agli adempimenti prescritti dalla normativa fiscale, previdenziale, assicurativa, di igiene e sicurezza del lavoro e per l'esecuzione a favore del lavoratore delle prestazioni cui ha diritto.

2) **Categorie particolari**: Nel corso di tale rapporto la scrivente società può venire a conoscenza di dati personali che il Regolamento definisce "categorie particolari di dati personali", in quanto gli stessi sono idonei a rivelare uno stato di salute (es. documentazione relativa ad un eventuale avviamento obbligatorio e quindi a una situazione di invalidità, certificati relativi alle assenze per malattia, maternità, infortunio, dati relativi all'idoneità a determinati lavori, eventuale presenza di soggetti inabili al lavoro, gli effetti del riconoscimento dell'assegno per il nucleo familiare), l'adesione ad un sindacato (assunzione di cariche sindacali, richiesta di trattenuta per quote di associazione sindacale), l'adesione ad un partito politico (richiesta di permessi o aspettativa per cariche pubbliche elettive, assenza retribuita per lo svolgimento dell'incarico di rappresentante di lista), convinzioni religiose (richiesta di fruizione, prevista dalla legge, di festività religiose).

I trattamenti di alcuni di questi dati sono effettuati per conto di Istituti previdenziali ed assistenziali, quali l'INPS e l'INAIL, ad esempio per il pagamento delle indennità economiche di malattia, di maternità, per inabilità temporanea provocata da infortunio e per la corresponsione dell'assegno per il nucleo familiare. Gli stessi Istituti hanno perciò il diritto di conoscere tali dati personali, anche sensibili, trattati dalla scrivente società.

3) **Comunicazione dei dati**: I dati personali relativi al trattamento in questione verranno comunicati, qualora ciò risulti necessario o comunque funzionale alla gestione del rapporto contrattuale e al perseguimento del legittimo interesse del titolare, ai seguenti soggetti: (eliminare le ipotesi non vere ed eventualmente integrare)

- a Pubbliche Amministrazioni, enti previdenziali e assistenziali, per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge, dal CCNL e dai regolamenti;
- alle Associazioni Sindacali per gli scopi previsti dalla normativa contrattuale e legislativa;
- agli Organismi paritetici;
- a Società del gruppo;
- ad Agenzie di viaggio per l'emissione di biglietti aerei, ferroviari e/o prenotazioni alberghiere in occasione di trasferte;
- a Società di Assicurazioni per la stipulazione di polizze a favore di dipendenti, nonché ai fini della riscossione del premio relativo alla polizza;
- agli Istituti bancari, di credito e/o finanziarie per l'accredito dello stipendio, cessione del quinto o pignoramento;
- ad enti e strutture di formazioni ai fini della formazione professionale;
- ad enti privati e studi professionali incaricati del trattamento di questioni inerenti al rapporto di lavoro (es. commercialista, consulente del lavoro);
- alle società terze con le quali sono in corso contratti di appalto nell'esecuzione del rapporto contrattuale (es. servizio mensa, sorveglianza privata, servizio trasporto);
- al medico competente incaricato della sorveglianza sanitaria ai sensi del Decreto Legislativo n. 81/2008;
- ……altro?

4) **Foto e riprese** (eventuale): la scrivente società potrebbe utilizzare immagini fotografiche dei propri dipendenti al fine di permettere una migliore identificazione sull'organigramma della società o sul badge di riconoscimento, con il solo scopo di

migliorare la sicurezza aziendale. La società dichiara ed assicura che la raccolta ed il trattamento di tali immagini sarà effettuato nella più rigorosa osservanza di quanto previsto dalla normativa vigente per la tutela della Privacy, anche per quanto riguarda la sicurezza dei dati, impegnandosi ad effettuarne il trattamento secondo le disposizioni di legge vigenti ed ad opera di soggetti appositamente incaricati, rispettando le finalità e le modalità del trattamento sopra dichiarate, nonché l'ambito di comunicazione e diffusione degli stessi e la natura dei dati e del loro conferimento.

5) **Acquisizione di immagini fotografiche o riprese video che ritraggano i dipendenti per attività di marketing e promozione della Società** (eventuale): la Società potrebbe realizzare, servizi fotografici, filmati, ed altri strumenti di comunicazione contenenti alcune immagini dei propri dipendenti e collaboratori. La Società scrivente ha interesse a poter utilizzare e divulgare tale materiale a fini promozionali, di marketing, anche attraverso canali di divulgazione quali ad esempio, a titolo esemplificativo ma non esaustivo, televisivi, web e social, pubblicazioni di vario genere, fiere e mostre, nell'UE (N.B. necessario il consenso)

6) **Videosorveglianza**: Si informa che è operativo un sistema di videosorveglianza lungo il perimetro dell'azienda ai soli fini della tutela del patrimonio aziendale. (da integrare se in azienda la videosorveglianza è estesa ad aree in relazione alle quali si è proceduto a sottoscrivere accordo sindacale/richiedere autorizzazione ispettiva)

7) **Telepass/carta credito aziendale** (eventuale): la società Le ha assegnato una autovettura/una carta di credito aziendale quali strumenti per agevolarLa nell'esecuzione del contratto di lavoro; la periodica rendicontazione dell'utilizzo di questi strumenti fornirà alla scrivente dati relativi alla posizione geografica del veicolo di lavoro e del relativo orario/ai luoghi e agli orari di utilizzo degli strumenti di pagamento assegnati.[1]

[1] Su segnalazione di un dipendente di una società che utilizza il sistema di localizzazione sulla propria flotta aziendale, il Garante per la protezione dei dati personali è intervenuto con provvedimento n. 396 del 28 giugno 2018 imponendo a un fornitore di sistemi GPS di incorporare nei propri prodotti funzionalità idonee a garantire che siano trattati, per impostazione predefinita, i soli dati personali necessari in relazione ad ogni specifica finalità del trattamento, nel rispetto del principio di minimizzazione e di quello di privacy by design e privacy by default.

8) Trasferimento dei dati personali: Nell'ambito dei rapporti contrattuali della scrivente società i dati personali potranno essere trasferiti al di fuori del territorio dell'Unione Europea (UE), anche mediante l'inserimento degli stessi in database gestiti da società terze, operanti per conto della scrivente società. La gestione dei database ed il trattamento dei dati personali sono vincolati alle finalità per cui gli stessi sono stati raccolti ed avvengono nel massimo rispetto della legge applicabile sulla protezione dei dati personali.

Tutte le volte in cui i Dati dovessero essere oggetto di trasferimento al di fuori dell'UE, la scrivente società adotterà ogni misura contrattuale idonea e necessaria a garantire un adeguato livello di protezione dei dati personali, inclusi - tra gli altri - gli accordi basati sulle clausole contrattuali standard per il trasferimento dei dati al di fuori dell'UE, approvate dalla Commissione Europea.

9) **Conservazione dei dati**: I dati personali raccolti in occasione della Sua assunzione e durante il rapporto di lavoro saranno conservati dalla scrivente società per il periodo ritenuto strettamente necessario a conseguire tali finalità.

I dati personali trattati, inoltre, potranno essere conservati anche a seguito della cessazione del rapporto di lavoro per un periodo compatibile con le esigenze connesse ad eventi e/o fatti successivi al rapporto di lavoro quali a titolo esemplificativo e non esaustivo la gestione di eventuali richieste connesse all'attività lavorativa da parte dello stesso dipendente e/o di terzi aventi diritto, nonché per gli ulteriori periodi corrispondenti ai termini di prescrizione delle azioni esercitabili da questi ultimi.

10) **Esercizio dei diritti**: All'interessato sono riconosciuti i seguenti diritti, fatto salvo quanto indicato al punto precedente in materia di conservazione dei dati personali:

- diritto di accesso, ossia il diritto di ottenere dalla scrivente società la conferma che sia o meno in corso il trattamento dei dati personali e, in tal caso, di ottenerne l'accesso;
- diritto di rettifica e cancellazione, ossia il diritto di ottenere la rettifica di dati personali inesatti e/o l'integrazione di dati personali incompleti o la cancellazione dei dati personali per motivi legittimi;
- diritto alla limitazione del trattamento, ossia il diritto a richiedere la sospensione del trattamento dei dati personali qualora sussistano motivi legittimi;

- diritto alla portabilità dei dati, ossia il diritto di ricevere in un formato strutturato, di uso comune e leggibile i dati personali, nonché il diritto di trasmettere i dati personali ad un altro titolare del trattamento;
- diritto di opposizione, ossia il diritto opporsi al trattamento dei dati personali qualora sussistano motivi legittimi;
- diritto di rivolgersi all'autorità per la protezione dei dati competente in caso di trattamento illecito dei dati personali.

L'interessato potrà esercitare i diritti sopra elencati inviando una richiesta scritta alla direzione Risorse Umane della scrivente società.

11) **Titolare del trattamento e Responsabile della protezione dei dati ("Data Protection Officer")**: Titolare del trattamento è la società scrivente _____, nella persona del legale rappresentante.

L'interessato può contattare il Data Protection Officer all'indirizzo email _____ (se nominato)

Luogo, _____

Il Titolare _____

L'interessato _____

(firma leggibile dell'interessato)

Acconsento Non Acconsento, all'utilizzo e alla divulgazione, a titolo gratuito, della mia immagine nei limiti ed in conformità all'informativa ricevuta (punto 5)

L'interessato _____

(firma leggibile dell'interessato)

Informativa Privacy per i Dipendenti Data di aggiornamento dell'informativa: xxxxx

Gentile sig…/ sigr.a., prima di procedere al trattamento dei suoi dati, Le sottoponiamo l'informativa Privacy prevista da xxxx (di seguito semplicemente Società), necessaria per la tutela dei suoi dati personali, secondo quanto previsto dalla normativa in materia.
Le informazioni di seguito riportate Le saranno utili per comprendere:

- quali sono i soggetti che trattano i suoi dati e come contattarli;
- come vengono analizzati i suoi dati e per quale motivo.

Contatti utili

xxxxx è la Società che tratta i suoi dati ed ai fini di Legge, è considerata Titolare del trattamento dei dati. In tale veste essa è responsa- bile di garantire l'applicazione delle misure organizzative e tecniche necessarie e adeguate alla protezione dei suoi dati. La sede della Società è in Via xxxx, xx xxx xxxx, xxx – Italia. E-mail: xxxxx.

Inoltre la Società ha nominato il Responsabile alla Protezione dei Dati (DPO) incaricato di garantire il rispetto delle norme per la tutela della sua Privacy, contattabile per questioni inerenti il trattamento dei suoi dati, al seguente indirizzo di posta elettronica: xxxxxx. Potrà trovare maggiori informazioni sui suoi diritti le nello spazio dedicato "I suoi diritti".

Informazioni sul trattamento

Le precisiamo che tutti i dati personali che Lei ci fornirà saranno trattati in conformità alla vigente normativa in materia di privacy, pertanto la Società si impegna a trattarli secondo principi di correttezza, liceità, trasparenza, nel rispetto delle finalità di seguito indicate, raccogliendoli nella misura necessaria ed esatta per il trattamento, consentendone l'utilizzo solo da personale allo scopo autorizzato e formato ed al fine di garantire la necessaria riservatezza delle informazioni fornite.

In particolare, la Società, raccoglie, registra, consulta e in generale tratta i suoi dati anagrafici e identificativi come ad esempio nome, cognome, indirizzo, telefono, e-mail, riferimenti bancari e di pagamento, necessari esclusivamente all'esecuzione delle finalità previste dal contratto.

La Società può usare le informazioni raccolte anche per lo svolgimento di alcune attività interne, quali ad esempio il controllo della propria sicurezza, la pianificazione del lavoro, etc. (cfr. quanto indicato nel registro dei trattamenti). Queste attività rientrano nell'ordinario esercizio dell'attività della Società e pertanto non è richiesto il consenso.

Durante il rapporto contrattuale, la Società pubblicherà alcuni suoi dati sul portale intranet aziendale, che costituisce uno strumento per l'esecuzione della prestazione lavorativa, oltre che idoneo a facilitare i contatti fra dipendenti. In tali casi, la base giuridica che legittima il trattamento è l'esecuzione del contratto di lavoro di cui Lei è parte.

Il trattamento dei dati suindicati è obbligatorio per l'esecuzione del contratto, pertanto il suo rifiuto renderà impossibile l'instaurazione del rapporto di lavoro con la Società.

La Società tratterà i suoi dati anche per adempiere ad obblighi o esercitare i diritti previsti dal diritto nazionale o dell'Unione Europea o da contratti collettivi in conformità con le leggi nazionali, come, a titolo esemplificativo, per la tutela della salute e sicurezza sul lavoro dei dipendenti. In tal caso, la base giuridica che legittima il trattamento è la necessità di adempiere obblighi legali cui è soggetto il titolare, nonché, per quanto concerne le categorie particolari di dati, assolvere gli obblighi ed esercitare i diritti del titolare o dell'interessato in materia di diritto del lavoro e della sicurezza e protezione sociale in conformità con quanto previsto nell'art. 9.2, lett. b) GDPR o per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente da parte del medico competente ai sensi dell'art. 9. co. 2, lett. h) e in conformità con quanto previsto dall'art. 9, co. 3 del GDPR.

Se necessario, i suoi dati saranno utilizzati anche per accertare, esercitare o difendere i diritti della Società in sede giudiziaria. In tal caso, la base giuridica che legittima il trattamento è l'interesse legittimo della Società.

Al fine di garantire la sicurezza di persone e beni, i suoi dati saranno trattati nel controllo degli accessi fisici, sia tramite badge, che tramite impianti di videosorveglianza (nel rispetto dell'art. 4 dello Statuto dei Lavoratori e s.m.i., le apparecchiature installate non sono preordinate al controllo a distanza dell'attività lavorativa).

Periodo di conservazione dei suoi dati La Società conserverà i suoi dati fino alla conclusione del contratto ed in seguito per un periodo di 10 anni, salvo il caso di rischio di malattie professionali che presentano un periodo di latenza, nel qual caso la conservazione dei docu- menti terrà conto del periodo di latenza scientificamente riconosciuto.

Nel rispetto di quanto previsto nel "Provvedimento in materia di videosorveglianza — 8 aprile 2010" del Garante per la Protezione dei dati personali, le immagini raccolte con il sistema di videosorveglianza sono conservate per un periodo pari a 7 giorni. Decorsi tali termini di conservazione, i suoi dati saranno distrutti o resi anonimi, compatibilmente con le procedure tecniche di cancellazione e backup.

Trasferimento e accesso ai suoi dati La Società — senza che sia necessario richiedere il suo specifico consenso — può comunicare i suoi dati personali ad una categoria di soggetti di seguito meglio indicati quali ad esempio:

- Società del Gruppo anche non presenti all'interno dell'UE (sulla base delle decisioni di adeguatezza della Commissione Europea o sulla base delle standard model clauses), al fine di svolgere attività di controllo e gestione del personale;

- soggetti terzi (a titolo indicativo, istituti di credito, studi professionali, consulenti, Società di assicurazione per la prestazione di servizi assicurativi, società di payroll, etc.) che svolgono attività in outsourcing per conto del Titolare, nella loro qualità di responsabili del trattamento;

- Autorità giudiziarie, società di assicurazione per la prestazione di servizi assicurativi, nonché a quei soggetti ai quali la comunicazione sia obbligatoria per legge. Detti soggetti tratteranno i dati nella loro qualità di autonomi titolari del trattamento.

I suoi diritti

Con riferimento ai dati trattati, la Società Le garantisce la possibilità di:

- ottenere la conferma dell'esistenza o meno dei dati personali che La riguardano e la loro copia in forma intelligibile;
- ottenere l'aggiornamento, la rettificazione o l'integrazione dei suoi dati;
- richiedere la cancellazione dei suoi dati, nei termini consentiti dalla normativa, oppure chiedere che siano anonimizzati;
- opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano;
- limitare il trattamento, in caso di violazione, richiesta di rettifica od opposizione;
- chiedere la portabilità dei dati trattati elettronicamente, forniti sulla base di consenso o contratto;
- revocare il consenso al trattamento dei suoi dati, qualora previsto.

A tale scopo, la Società ha previsto sul sito internet una specifica sezione in cui può scaricare i moduli. In alternativa La invita a recuperare i moduli inviando una mail al seguente indirizzo: xxxxxx per presentare le sue richieste in maniera gratuita.

La informiamo che la Società si impegna a rispondere alle sue richieste entro il termine di un mese, salvo caso di particolare complessità, per cui potrebbe impiegare massimo 3 mesi. In ogni caso, la Società provvederà a spiegare il motivo dell'attesa entro un mese dalla sua richiesta.

L'esito della sua richiesta Le verrà fornito per iscritto, in formato elettronico o cartaceo. Nel caso chieda la rettifica, la cancellazione nonché la limitazione del trattamento, la Società si impegna a comunicare gli esiti delle sue richieste a ciascuno dei destinatari dei suoi dati, salvo che ciò risulti impossibile o implichi un o sforzo sproporzionato.

Si ricorda che la revoca del consenso, qualora questa fosse la base giuridica del trattamento, non pregiudica la liceità del trattamento basato sul consenso, prima della revoca.

La Società specifica che Le potrà essere richiesto un eventuale contributo, qualora le sue domande risultino manifestamente infondate, eccessive o ripetitive; a tal proposito, la Società si è dotata di un registro per tracciare le sue richieste di intervento.

Luogo / data

Privacy Notice for Employees

Updated on: xxxx

Dear Employee, before proceeding with the processing of your data, please read the Privacy notice provided by xxxxx (hereinafter "the Company"), necessary for the protection of your personal data, as required by privacy legislation.
The information below will be useful to help you understand:

- who will process your data and how to contact them;
- how your data will be analysed and for what reason.

Useful contacts

xxxx is the Company that processes your data and for the purposes of the law, is the Data Controller. In this capacity it is responsible for ensuring the application of necessary and adequate organisational and technical measures to protect your data. The Company is based in Via xxxx, xx xxx xxxx, xxx - xxx. E-mail: xxxxx.

Additionally, the Company has appointed a Data Protection Officer (DPO) who will be responsible for ensuring compliance with the rules for protecting your Privacy and who can be contacted for matters concerning personal data processing, at the following e-mail address: xxxxx. You can find more information about your rights in the "Your rights" section.

Information on data processing

Please note that all the personal data provided by you will be processed in accordance with current legislation on privacy. Therefore the Company undertakes to process said data in accordance with the principles of fairness, lawfulness and transparency, in compliance with the purposes set out below, collecting said data only for specified and necessary purposes. Only authorised and properly trained personnel will be allowed the use of said data in order to guarantee the necessary confidentiality of the information provided.

Specifically, the Company collects, records, consults and generally processes your personal and identifying data such as name, surname, address, telephone number, e-mail address, bank and payment details, which are necessary exclusively for the execution of the contract.

The Company may also use the information collected for the performance of certain internal activities, such as the control of one's own safety, work planning, etc. (Please refer to the information on the record of processing activities). These activities fall within ordinary Company operations and therefore do not require consent.

During the contractual relationship, the Company will publish your data on the company Intranet, which is one of the tools necessary to perform the work, as well as being suitable for facilitating contact among employees. In these cases, the lawfulness of the processing is based on execution of your employment contract.

The processing of the aforementioned data is mandatory for execution of the contract and therefore refusing to allow processing will make it impossible to work for the Company.

The Company will also process your data to fulfil obligations or exercise its rights provided for by national or European Union law or by collective agreements in accordance with national laws, such as, for workplace health and safety. In this case, the lawfulness of the processing is based on the need to comply with the legal obligations of the data controller and for specific data categories, to fulfil the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in line with the provisions of art. 9.2, lett. b) of the GDPR or for preventive or occupational medicine, for the assessment of the working capacity of the employee by the Company Doctor in line with the provisions of art. 9.2, lett. h) of the GDPR and in compliance with the provisions of art. 9.3 of the GDPR.

If necessary, your data will also be used to ascertain, exercise or defend the rights of the Company in court. In this case, the lawfulness of the processing is based on protecting the legitimate interest of the Company.

In order to guarantee the safety of people and assets, your data will be processed during the control of physical access, both by badge and through video surveillance systems (in compliance with Article 4 of the Workers' Statute and subsequent amendments, video equipment installed will not be used to monitor employees while working).

Retention period of personal data

The Company will retain your data for the duration of the employment contract and thereafter for a period of 10 years, unless there is a risk of occupational diseases with a latency period, in which case documents will be saved taking into account the scientifically acknowledged latency period.

In compliance with the "Video Surveillance - Guidelines by the Italian DPA - 8 April 2010" issued by the Personal Data Protection Authority, images collected with the video surveillance system are kept for a period of 7 days. Once these deadlines have passed, your data will be destroyed or made anonymous, in line with the technical procedures for cancellation and backup.

Transfer and access to personal data

The Company - without needing your specific consent - may communicate your personal data to other subjects, the categories of which are described in detail below, for example:

- xxxx Group companies, even if not located in the EU (based on the adequacy decisions by the European Commission or on the basis of standard model clauses), in order to carry out personnel management and control activities;

- third parties (for example credit institutes, professional firms, consultants, insurance companies for the provision of insurance services, payroll companies, etc.) who carry out outsourcing activities on behalf of the Data Controller, in their capacity as Data Processors;

- Judicial authorities, insurance companies for the provision of insurance services, as well as those subjects to whom communication is required by law. These subjects will process the data in their capacity as independent Data Controllers.

Your rights

With reference to the data processed, the Company guarantees that you have the right:

- to receive confirmation of the existence of your personal data and to receiving it in an intelligible form.
- to obtain the updating, rectification or integration of your data;
- to request the deletion of your data, within the terms permitted by law, or request the pseudonymisation of your data;
- to object, in whole or in part, for legitimate reasons, to the processing of your personal data;
- to restrict the processing, in case of violation, request for rectification or opposition;
- to request the portability of electronically processed data, provided on the basis of consent or contract;
- to withdraw consent for the processing of your data, if required.

For this purpose, the Company has provided a specific section on the website where you can download the necessary forms. Alternatively, you may request the forms by sending an email to the following address: xxxxx to submit your requests free of charge.

Please be informed that the Company shall undertake to respond to your requests within one month, except in cases of particular complexity, so it may take up to 3 months. In any case, the Company will notify you of any delay within one month of your request.

You will receive your reply in writing, either digitally or on hard copy. Should you request the rectification, the cancellation and the limitation of data processing, the Company undertakes to notify each recipient of your data of your request, unless this proves to be impossible or involves a disproportionate effort.

Please remember that the withdrawal of consent, if the lawfulness of processing was based on consent, does not affect the lawfulness of the processing, before revocation of consent.

Please be advised that you may be asked for payment, if your applications are manifestly unfounded, excessive or repetitive; to this end, the Company keeps a register to track your requests for action.

City/Date

1.2 Informativa Privacy per gli Stagisti
Data di aggiornamento dell'informativa: xxxx

Gentile sig…/ sigr.a., prima di procedere al trattamento dei suoi dati, Le sottoponiamo l'informativa Privacy prevista da xxxxx (di se- guito semplicemente Società), necessaria per la tutela dei suoi dati personali, secondo quanto previsto dalla normativa in materia.
Le informazioni di seguito riportate Le saranno utili per comprendere:
•quali sono i soggetti che trattano i suoi dati e come contattarli;
•come vengono analizzati i suoi dati e per quale motivo.

Contatti utili

xxxx è la Società che tratta i suoi dati ed ai fini di Legge, è considerata Titolare del trattamento dei dati. In tale veste essa è responsabile di garantire l'applicazione delle misure organizzative e tecniche necessarie e adeguate alla protezione dei suoi dati. La sede della Società è in Via xxx, xxx xxx xxxx, xxx – xxx. E-mail: xxxxx.

Inoltre la Società ha nominato il Responsabile alla Protezione dei Dati (DPO) incaricato di garantire il rispetto delle norme per la tutela della sua Privacy, contattabile per questioni inerenti il trattamento dei suoi dati, al seguente indirizzo di posta elettronica: xxxxx. Potrà trovare maggiori informazioni sui suoi diritti le nello spazio dedicato "I suoi diritti".

Informazioni sul trattamento

Le precisiamo che tutti i dati personali che Lei ci fornirà saranno trattati in conformità alla vigente normativa in materia di privacy, pertanto la Società si impegna a trattarli secondo principi di correttezza, liceità, trasparenza, nel rispetto delle finalità di seguito indicate, raccogliendoli nella misura necessaria ed esatta per il trattamento, consentendone l'utilizzo solo da personale allo scopo autorizzato e formato ed al fine di garantire la necessaria riservatezza delle informazioni fornite.

In particolare, la Società, raccoglie, registra, consulta e in generale tratta i suoi dati anagrafici e identificativi come ad esempio nome, cognome, indirizzo, telefono, e-mail, riferimenti bancari e di pagamento, necessari esclusivamente all'esecuzione delle finalità previste dal tirocinio formativo.

La Società può usare le informazioni raccolte anche per lo svolgimento di alcune attività interne, quali ad esempio il controllo della propria sicurezza, la pianificazione delle attività connesse al progetto formativo, etc. (cfr. quanto indicato nel registro dei trattamenti).

Queste attività rientrano nell'ordinario esercizio dell'attività della Società e pertanto non è richiesto il consenso.

Durante il rapporto contrattuale, la Società potrebbe pubblicare alcuni suoi dati sul portale intranet aziendale, che costituisce uno strumento per l'esecuzione del tirocinio formativo di cui Lei è parte. In tali casi, la base giuridica che legittima il trattamento è l'esecuzione del progetto formativo.

Il trattamento dei dati suindicati è obbligatorio per l'esecuzione del progetto formativo, pertanto il suo rifiuto renderà impossibile lo svolgimento di tale progetto.

La Società tratterà i suoi dati anche per adempiere ad obblighi o esercitare i diritti previsti dal diritto nazionale o dell'Unione Europea come, a titolo esemplificativo, per la tutela della salute e sicurezza sul lavoro. In tal caso, la base giuridica che legittima il trattamento è la necessità di adempiere obblighi legali cui è soggetto il titolare, nonché, per quanto concerne le categorie particolari di dati, assolvere gli obblighi ed esercitare i diritti del titolare o dell'interessato in materia di sicurezza e protezione sociale in conformità con quanto previsto nell'art. 9.2, lett. b) GDPR .

Se necessario, i suoi dati saranno utilizzati anche per accertare, esercitare o difendere i diritti della Società in sede giudiziaria. In tal caso, la base giuridica che legittima il trattamento è l'interesse legittimo della Società.

Al fine di garantire la sicurezza di persone e beni, i suoi dati saranno trattati nel controllo degli accessi fisici, sia tramite badge, che tramite impianti di videosorveglianza (nel rispetto dell'art. 4 dello Statuto dei Lavoratori e s.m.i.).

Periodo di conservazione dei suoi dati La Società conserverà i suoi dati fino alla conclusione del progetto formativo ed in seguito per un periodo di 10 anni.

Nel rispetto di quanto previsto nel "Provvedimento in materia di videosorveglianza — 8 aprile 2010" del Garante per la Protezione dei dati personali, le immagini raccolte con il sistema di videosorveglianza sono conservate per un periodo pari a 7 giorni. Decorsi tali termini di conservazione, i suoi dati saranno distrutti o resi anonimi, compatibilmente con le procedure tecniche di cancellazione e backup.

Trasferimento e accesso ai suoi dati

La Società — senza che sia necessario richiedere il suo specifico consenso — può comunicare i suoi dati personali ad una categoria di soggetti di seguito meglio indicati quali ad esempio:

- Società del Gruppo anche non presenti all'interno dell'UE (sulla base delle decisioni di adeguatezza della Commissione Europea o sulla base delle standard model clauses), al fine di svolgere attività connesse al progetto formativo;

- soggetti terzi (a titolo indicativo, istituti di credito, enti di formazione, consulenti, Società di assicurazione per la prestazione di servizi assicurativi, società di payroll, etc.) che svolgono attività in outsourcing per conto del Titolare, nella loro qualità di responsabili del trattamento;

- Autorità giudiziarie, società di assicurazione per la prestazione di servizi assicurativi, nonché a quei soggetti ai quali la comunicazione sia obbligatoria per legge. Detti soggetti tratteranno i dati nella loro qualità di autonomi titolari del trattamento.

I suoi diritti

Con riferimento ai dati trattati, la Società Le garantisce la possibilità di:

•ottenere la conferma dell'esistenza o meno dei dati personali che La riguardano e la loro copia in forma intelligibile;
•ottenere l'aggiornamento, la rettificazione o l'integrazione dei suoi dati;
•richiedere la cancellazione dei suoi dati, nei termini consentiti dalla normativa, oppure chiedere che siano anonimizzati;
• opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano;
•limitare il trattamento, in caso di violazione, richiesta di rettifica od opposizione;
•chiedere la portabilità dei dati trattati elettronicamente, forniti sulla base di consenso o contratto;
•revocare il consenso al trattamento dei suoi dati, qualora previsto.

A tale scopo, la Società ha previsto sul sito internet una specifica sezione in cui può scaricare i moduli. In alternativa La invita a recuperare i moduli inviando una mail al seguente indirizzo: xxxxx per presentare le sue richieste in maniera gratuita.

La informiamo che la Società si impegna a rispondere alle sue richieste entro il termine di un mese, salvo caso di particolare complessità, per cui potrebbe impiegare massimo 3 mesi. In ogni caso, la Società provvederà a spiegare il motivo dell'attesa entro un mese dalla sua richiesta.

L'esito della sua richiesta Le verrà fornito per iscritto, in formato elettronico o cartaceo. Nel caso chieda la rettifica, la cancellazione nonché la limitazione del trattamento, la Società si impegna a comunicare gli esiti delle sue richieste a ciascuno dei destinatari dei suoi dati, salvo che ciò risulti impossibile o implichi un o sforzo sproporzionato.

Si ricorda che la revoca del consenso, qualora questa fosse la base giuridica del trattamento, non pregiudica la liceità del trattamento basato sul consenso, prima della revoca.

La Società specifica che Le potrà essere richiesto un eventuale contributo, qualora le sue domande risultino manifestamente infondate, eccessive o ripetitive; a tal proposito, la Società si è dotata di un registro per tracciare le sue richieste di intervento.

Luogo / data

Privacy Notice for Interns

Updated on: xxxx

Dear , before proceeding with the processing of your data, please read the Privacy notice provided by xxxxx (hereinafter “the Com- pany”), necessary for the protection of your personal data, as required by privacy legislation.
The information below will be useful to help you understand:
• who will process your data and how to contact them;
• how your data will be analysed and for what reason.

Useful contacts

xxxxx is the Company that processes your data and for the purposes of the law, is the Data Controller. In this capacity it is responsible for ensuring the application of necessary and adequate organisational and technical measures to protect your data. The Company is based in Via xxx, xxx xxxx xxxx, xxx - xxx. E-mail: xxxx.

Additionally, the Company has appointed a Data Protection Officer (DPO) who will be responsible for ensuring compliance with the rules for protecting your Privacy and who can be contacted for matters concerning personal data processing, at the following e-mail address: xxxxx. You can find more information about your rights in the "Your rights" section.

Information on data processing

Please note that all the personal data provided by you will be processed in accordance with current legislation on privacy. Therefore the Company undertakes to process said data in accordance with the principles of fairness, lawfulness and transparency, in compliance with the purposes set out below, collecting said data only for specified and necessary purposes. Only authorised and properly trained personnel will be allowed the use of said data in order to guarantee the necessary confidentiality of the information provided.

Specifically, the Company collects, records, consults and generally processes your personal and identifying data such as name, surname, address, telephone number, e-mail address, bank and payment details, which are necessary exclusively for the execution of the internship.

The Company may also use the information collected for the performance of certain internal activities, such as the control of one's own safety, work planning related to the internship program, etc.

(Please refer to the information on the record of processing activities). These activities fall within ordinary Company operations and therefore do not require consent.

During the contractual relationship, the Company could publish your data on the company Intranet, which is one of the tools necessary to perform the internship program. In these cases, the lawfulness of the processing is based on execution of your internship contract.

The processing of the aforementioned data is mandatory for the execution of the internship and therefore refusing to allow processing will make it impossible to perform the internship program.

The Company will also process your data to fulfil obligations or exercise its rights provided for by national or European Union law, such as, for workplace health and safety. In this case, the lawfulness of the processing is based on the need to comply with the legal obligations of the data controller and for specific data categories, to fulfil the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in line with the provisions of art. 9.2, lett. b) of the GDPR.

If necessary, your data will also be used to ascertain, exercise or defend the rights of the Company in court. In this case, the lawfulness of the processing is based on protecting the legitimate interest of the Company.

In order to guarantee the safety of people and assets, your data will be processed during the control of physical access, both by badge and through video surveillance systems (in compliance with Article 4 of the Workers' Statute and subsequent amendments).

Retention period of personal data

The Company will retain your data for the duration of the internship contract and thereafter for a period of 10 years.

In compliance with the "Video Surveillance - Guidelines by the Italian DPA - 8 April 2010" issued by the Personal Data Protection Authority, images collected with the video surveillance system are kept for a period of 7 days. Once these deadlines have passed, your data will be destroyed or made anonymous, in line with the technical procedures for cancellation and backup.

Transfer and access to personal data

The Company - without needing your specific consent - may communicate your personal data to other subjects, the categories of which are described in detail below, for example:

- xxxx Group companies, even if not located in the EU (based on the adequacy decisions by the European Commission or on the basis of standard model clauses), in order to carry out personnel management and control activities related to the internship program;

- third parties (for example credit institutes, training agencies, consultants, insurance companies for the provision of insurance services, payroll companies, etc.) who carry out outsourcing activities on behalf of the Data Controller, in their capacity as Data Processors;

- Judicial authorities, insurance companies for the provision of insurance services, as well as those subjects to whom communication is required by law. These subjects will process the data in their capacity as independent Data Controllers.

Your rights

With reference to the data processed, the Company guarantees that you have the right:

- to receive confirmation of the existence of your personal data and to receiving it in an intelligible form.
- to obtain the updating, rectification or integration of your data;
- to request the deletion of your data, within the terms permitted by law, or request the pseudonymisation of your data;
- to object, in whole or in part, for legitimate reasons, to the processing of your personal data;
- to restrict the processing, in case of violation, request for rectification or opposition;
- to request the portability of electronically processed data, provided on the basis of consent or contract;
- to withdraw consent for the processing of your data, if required.

For this purpose, the Company has provided a specific section on the website where you can download the necessary forms. Alternatively, you may request the forms by sending an email to the following address: xxxx to submit your requests free of charge.

Please be informed that the Company shall undertake to respond to your requests within one month, except in cases of particular complexity, so it may take up to 3 months. In any case, the Company will notify you of any delay within one month of your request.

You will receive your reply in writing, either digitally or on hard copy. Should you request the rectification, the cancellation and the limita- tion of data processing, the Company undertakes to notify each recipient of your data of your request, unless this proves to be impossible or involves a disproportionate effort.

Please remember that the withdrawal of consent, if the lawfulness of processing was based on consent, does not affect the lawfulness of the processing, before revocation of consent.

Please be advised that you may be asked for payment, if your applications are manifestly unfounded, excessive or repetitive; to this end, the Company keeps a register to track your requests for action.

City/Date

1.3 Informativa Privacy per i Candidati Data di aggiornamento dell'informativa: xxx

Gentile Candidato, prima di procedere al trattamento dei suoi dati, Le sottoponiamo l'informativa Privacy prevista da xxxxxx (di segui- to semplicemente Società), necessaria per la tutela dei suoi dati personali, secondo quanto previsto dalla normativa in materia.
Le informazioni di seguito riportate Le saranno utili per comprendere:

- quali sono i soggetti che trattano i suoi dati e come contattarli;
- come vengono analizzati i suoi dati e per quale motivo.

Contatti utili

xxxx è la Società che tratta i suoi dati ed ai fini di Legge, è considerata Titolare del trattamento dei dati. In tale veste essa è responsabile di garantire l'applicazione delle misure organizzative e tecniche necessarie e adeguate alla protezione dei suoi dati. La sede della Società è in Via xxx, xx xx xx, xxxx – xxxxx. E-mail: xxxxxxxx.

Inoltre la Società ha nominato il Responsabile alla Protezione dei Dati (DPO) incaricato di garantire il rispetto delle norme per la tutela della sua Privacy, contattabile per questioni inerenti il trattamento dei suoi dati, al seguente indirizzo di posta elettronica: xxx.

Potrà trovare maggiori informazioni sui suoi diritti le nello spazio dedicato "I suoi diritti".

Informazioni sul trattamento

Le precisiamo che tutti i dati personali che Lei ci fornirà saranno trattati in conformità alla vigente normativa in materia di privacy, pertanto la Società si impegna a trattarli secondo principi di correttezza, liceità, trasparenza, nel rispetto delle finalità di seguito indicate, raccogliendoli nella misura necessaria ed esatta per il trattamento, consentendone l'utilizzo solo da personale allo scopo autorizzato e formato ed al fine di garantire la necessaria riservatezza delle informazioni fornite.

In particolare, la Società raccoglie, registra, consulta e in generale tratta i suoi dati contenuti nel CV necessari esclusivamente al processo di candidatura online. La base giuridica del trattamento è il consenso dell'interessato.

La Società tratterà i suoi dati per le seguenti finalità:

1) attività di ricerca e selezione del personale;
2) creazione di una banca dati funzionale al perseguimento di tale finalità;
3) attività precontrattuali relative all'in - teresse da Lei dichiaratoci di instaurare un rapporto di lavoro.

La Società, sulla base dei propri legittimi interessi, può usare altresì le informazioni raccolte per far valere o difendere un diritto in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa dell'Unione Europea, laddove insorga la necessità.

Periodo di conservazione dei suoi dati

La Società cancellerà i suoi dati, raccolti nel corso della registrazione, dopo un anno dall'ultimo suo accesso al sistema.

Le consigliamo cortesemente di mantenere la candidatura aggiornata.

Trasferimento e accesso ai suoi dati

La Società — senza che sia necessario richiedere il suo specifico consenso — può comunicare i suoi dati personali a categorie di soggetti di seguito meglio indicati quali ad esempio:

- Società del Gruppo, anche non presenti all'interno dell'UE (sulla base delle decisioni di adeguatezza della Commissione Europea o sulla base delle standard model clauses), al fine di svolgere le attività previste dal processo di candidatura;

- soggetti terzi (a titolo indicativo, istituti di credito, studi professionali, consulenti, Società di assicurazione per la prestazione di servizi assicurativi, etc.) che svolgono attività in outsourcing per conto del Titolare;

- Autorità giudiziarie, Società di assicurazione per la prestazione di servizi assicurativi, nonché quei soggetti ai quali la comunicazione è obbligatoria per legge. Detti soggetti tratteranno i dati nella loro qualità di autonomi tito- lari del trattamento.

I suoi diritti

Con riferimento ai dati trattati, la Società Le garantisce la possibilità di:

- ottenere la conferma dell'esistenza o meno dei dati personali che La riguardano e la loro copia in forma intelligibile;
- ottenere l'aggiornamento, la rettificazione o l'integrazione dei suoi dati;
- richiedere la cancellazione dei suoi dati, nei termini consentiti dalla normativa, oppure chiedere che siano anonimizzati;
- opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano;
- limitare il trattamento, in caso di violazione, richiesta di rettifica od opposizione;
- chiedere la portabilità dei dati trattati elettronicamente, forniti sulla base di consenso o contratto;
- revocare il consenso al trattamento dei suoi dati, qualora previsto.

A tale scopo, la Società ha previsto sul sito internet una specifica sezione in cui può scaricare i moduli. In alternativa La invita a recuperare i moduli inviando una mail al seguente indirizzo: xxxxxxxx per presentare le sue richieste in maniera gratuita.

La informiamo che la Società si impegna a rispondere alle sue richieste entro il termine di un mese, salvo caso di particolare complessità, per cui potrebbe impiegare massimo 3 mesi. In ogni caso, la Società provvederà a spiegarLe il motivo dell'attesa entro un mese dalla sua richiesta.

L'esito della sua richiesta Le verrà fornito per iscritto, in formato elettronico o cartaceo. Nel caso chieda la rettifica, la cancellazione nonché la limitazione del trattamento, la Società si impegna a comunicare gli esiti delle sue richieste a ciascuno dei destinatari dei suoi dati, salvo che ciò risulti impossibile o implichi uno sforzo sproporzionato.

Si ricorda che la revoca del consenso, qualora questa fosse la base giuridica del trattamento, non pregiudica la liceità del trattamento basato sul consenso, prima della revoca.

La Società specifica che Le potrà essere richiesto un eventuale contributo, qualora le sue domande risultino manifestamente infondate, eccessive o ripetitive; a tal proposito, la Società si è dotata di un registro per tracciare le sue richieste di intervento.

Luogo/data

Privacy Notice for Candidates

Updated on: xxxx

Dear Candidate, before proceeding with the processing of your personal data, please read the Privacy notice provided by xxxxx (hereinafter "the Company"), necessary for the protection of your personal data, as required by privacy legislation.
The information below will be useful to help you understand:

- who will process your data and how to contact them;
- how your data will be analysed and for what reason.

Useful contacts

xxxx is the Company that processes your data and for the purposes of the law, is the Data Controller. In this capacity it is responsible for ensuring the application of necessary and adequate organisational and technical measures to protect your data. The Company is based in Via xxxx, xxx xxx xxx, xxx - xxxx. E-mail: xxxxx

Additionally, the Company has appointed a Data Protection Officer (DPO) who will be responsible for ensuring compliance with the laws protecting your Privacy and who can be contacted for matters concerning personal data processing, at the following e-mail address: xxxxxx

You can find more information about your rights in "Your rights" section.

Information on data processing

Please note that all the personal data provided by you will be processed in accordance with current legislation on privacy. Therefore the Company undertakes to process said data in accordance with the principles of fairness, lawfulness and transparency, in compliance with the purposes set out below, collecting said data only for specified and necessary purposes. Only authorised and properly trained personnel will be allowed the use of said data in order to guarantee the necessary confidentiality of the information provided.

Specifically, the Company will collect, record, consult and generally process your data provided in the CV which are necessary exclusively for the online application process. Processing of the data is lawful only with consent from the data subject.

The Company will process your data for the following purposes:

1) recruitment and selection of personnel;

2) creation of an operational database to attain this objective;

3) pre-contractual activities relating to your interest in being employed by the Company.

The Company, for its own legitimate interests, may also use the information gathered to assert or defend a right in court or in arbitration and conciliation procedures in the cases provided for by law, by European Union law, where necessary.

Retention period of personal data

The Company will delete your personal data, collected during registration, one year after the last time you access the system.

We kindly advise you to keep your application updated.

Transfer and access to your data

The Company - without needing your specific consent - may communicate your personal data to other subjects, the categories of which are described in detail below, for example:

- xxxxx Group companies, even if not located in the EU (based on the adequacy decisions by the European Commission or on the basis of standard model clauses), in order to carry out the activities required by the application process;

- third parties (for example credit institutes, professional firms, consultants, insurance companies for the provision of insurance services, etc.) who carry out outsourcing activities on behalf of the Data Controller;

- Judicial authorities, Insurance companies for the provision of insurance services, as well as those subjects to whom communication is required by law. These subjects will process the data in their capacity as independent Data Controllers.

Your rights

With reference to the data processed, the Company guarantees that you have the right:

- to receive confirmation of the existence of your personal data and to receive them in an intelligible form.
- to obtain the updating, rectification or integration of your data;
- to request the deletion of your data, within the terms permitted by law, or request the pseudonymisation of your data;
- to object, in whole or in part, for legitimate reasons, to the processing of your personal data;
- to restrict the processing, in case of violation, request for rectification or opposition;
- to request the portability of electronically processed data, provided on the basis of consent or contract;
- to withdraw consent for the processing of your data, if required.

For this purpose, the Company has provided a specific section on the website where you can download the necessary forms. Alternatively, you may request the forms by sending an email to the following address: xxxxx to submit your requests free of charge.

Please be informed that the Company shall undertake to respond to your requests within one month, except in cases of particular complexity, so it may take up to 3 months. In any case, the Company will notify you of any delay within one month of your request.

You will receive your reply in writing, either digitally or on hard copy. Should you request the rectification, the cancellation and / or the limitation of data processing, the Company undertakes to notify each recipient of your data of your request, un- less this proves to be impossible or involves a disproportionate effort.

Please remember that the withdrawal of consent, if the lawfulness of processing was based on consent, does not affect the lawfulness of the processing, before revocation of consent.

Please be advised that you may be asked for payment, if your applications are manifestly unfounded, excessive or repetitive; to this end, the Company keeps a register to track your requests for action.

City/date

1.4 Informativa Privacy per gli ex Dipendenti
Data di aggiornamento dell'informativa: xxxxx

Gentile_____, considerata l'imminente risoluzione del suo contratto di lavoro, nonché la conseguente uscita dalla Società, prima di procedere al trattamento dei suoi dati, Le sottoponiamo l'informativa Privacy prevista da xxxxx (di seguito semplice- mente Società), necessaria per la tutela dei suoi dati personali, secondo quanto previsto dalla normativa in materia.
Le informazioni di seguito riportate Le saranno utili per comprendere:

- quali sono i soggetti che trattano i suoi dati e come contattarli;
- come vengono analizzati i suoi dati e per quale motivo.

Contatti utili

xxxx è la Società che tratta i suoi dati ed ai fini di Legge, è considerata Titolare del trattamento dei dati. In tale veste essa è responsa- bile di garantire l'applicazione delle misure organizzative e tecniche necessarie e adeguate alla protezione dei suoi dati. La sede della Società è in Via xxx, xxx xxx xxx, xxx – xx. E-mail: xxxxxx.

Inoltre la Società ha nominato il Responsabile alla Protezione dei Dati (DPO) incaricato di garantire il rispetto delle norme per la tutela della sua Privacy, contattabile per questioni inerenti il trattamento dei suoi dati, al seguente indirizzo di posta elettronica: xxxx. Potrà trovare maggiori informazioni sui suoi diritti le nello spazio dedicato "I suoi diritti".

Informazioni sul trattamento

Le precisiamo che tutti i dati personali che Lei ci ha fornito e/o ci fornirà saranno trattati in conformità alla vigente normativa in materia di privacy, pertanto la Società si impegna a trattarli secondo principi di correttezza, liceità, trasparenza, nel rispetto delle finalità di seguito indicate, raccogliendoli nella misura necessaria ed esatta per il trattamento, consentendone l'utilizzo solo da personale allo scopo autorizzato e formato ed al fine di garantire la necessaria riservatezza delle informazioni fornite.

In particolare, la Società conserva i dati necessari esclusivamente per adempiere a prescrizioni di legge, nonché alla tutela del diritto alla difesa della Società e li consulterà nel caso in cui dovessero sorgere specifiche esigenze di legge, richieste di Autorità nonché procedimenti giudiziari o amministrativi.

La Società, anche mediante controlli periodici, verificherà costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati conservati rispetto al rapporto, alla prestazione o all'incarico cessato, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.

In particolare, la Società conserverà i suoi dati per le seguenti finalità:

1) adempiere a prescrizioni di legge, in particolare ad obblighi in materia fiscale-amministrativa. La base giuridica del trattamento è la normativa applicabile;

2) rispondere a richieste di Autorità, nonché far valere o difendere un diritto in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e conciliazione nei casi previsti dalle leggi, dalla normativa dell'Unione Europea, dai regolamenti o dai contratti collettivi. La base giuridica del trattamento è il contratto che è intercorso tra Lei e la Società.

Periodo di conservazione dei suoi dati

I suoi dati saranno conservati secondo i seguenti criteri:

- per adempimenti di legge e per finalità fiscali-amministrative inerenti l'attività delle Società, i dati saranno conservati entro il limite massimo di accertamento previsto dalla normativa di settore;

- per adempiere a richieste di Autorità, nonché far valere o difendere un diritto in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa dell'Unione europea, dai regolamenti o dai contratti collettivi, per il periodo strettamente necessario al loro perseguimento, entro i termini di prescrizione dei relativi diritti.

Trasferimento e accesso ai suoi dati

La Società — senza che sia necessario richiedere il suo specifico consenso — può comunicare i suoi dati personali a categorie di soggetti di seguito meglio indicati, quali ad esempio:

- soggetti terzi (a titolo indicativo, istituti di credito, studi professionali, consulenti, Società di assicurazione per la prestazione di servizi assicurativi, società di payroll, etc.) che svolgono attività in outsourcing per conto del Titolare, nella loro qualità di responsabili del trattamento;

- Autorità giudiziarie, società di assicurazione per la prestazione di servizi assicurativi, nonché a quei soggetti ai quali la comunicazione sia obbligatoria per legge. Detti soggetti tratteranno i dati nella loro qualità di autonomi titolari del trattamento.

I suoi diritti

Con riferimento ai dati trattati, la Società Le garantisce la possibilità di:

- ottenere la conferma dell'esistenza o meno dei dati personali che La riguardano e la loro copia in forma intelligibile;
- ottenere l'aggiornamento, la rettificazione o l'integrazione dei suoi dati;
- richiedere la cancellazione dei suoi dati, nei termini consentiti dalla normativa, oppure chiedere che siano anonimizzati;
- opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano;
- limitare il trattamento, in caso di violazione, richiesta di rettifica od opposizione;
- chiedere la portabilità dei dati trattati elettronicamente, forniti sulla base di consenso o contratto;
- revocare il consenso al trattamento dei suoi dati, qualora previsto.

A tale scopo, la Società ha previsto sul sito internet una specifica sezione in cui può scaricare i moduli. In alternativa La invita a recuperare i moduli inviando una mail al seguente indirizzo: xxxx per presentare le sue richieste in maniera gratuita.

La informiamo che la Società si impegna a rispondere alle sue richieste entro il termine di un mese, salvo caso di particolare complessità, per cui potrebbe impiegare massimo 3 mesi. In ogni caso, la Società provvederà a spiegare il motivo dell'attesa entro un mese dalla sua richiesta.

L'esito della sua richiesta Le verrà fornito per iscritto, in formato elettronico o cartaceo. Nel caso chieda la rettifica, la cancellazione nonché la limitazione del trattamento, la Società si impegna a comunicare gli esiti delle sue richieste a ciascuno dei destinatari dei suoi dati, salvo che ciò risulti impossibile o implichi un o sforzo sproporzionato.

Si ricorda che la revoca del consenso, qualora questa fosse la base giuridica del trattamento, non pregiudica la liceità del trattamento basato sul consenso, prima della revoca.

La Società specifica che Le potrà essere richiesto un eventuale contributo, qualora le sue domande risultino manifestamente infondate, eccessive o ripetitive; a tal proposito, la Società si è dotata di un registro per tracciare le sue richieste di intervento.

Privacy Notice for former Employees

Updated on: xxxxx

Dear_____, in consideration of the imminent termination of your employment contract and your departure from the Company, before proceeding with the processing of your data, please read the Privacy notice provided by xxxx (hereinafter “the Company”), necessary for the protection of your personal data, as required by privacy legislation.
The information below will be useful to help you understand:

- who will process your data and how to contact them;
- how your data will be analysed and for what reason.

Useful contacts

xxxx is the Company that processes your data and for the purposes of the law, is the Data Controller. In this capacity it is responsible for ensuring the application of necessary and adequate organisational and technical measures to protect your data. The Company is based in Via xxx, xx xxx xxx, xx - xxx. E-mail: xxx.

Additionally, the Company has appointed a Data Protection Officer (DPO) who will be responsible for ensuring compliance with the rules for protecting your Privacy and who can be contacted for matters concerning personal data processing, at the following e-mail address: xxxx. You can find more information about your rights in the "Your rights" section.

Information on data processing

Please note that all the personal data provided by you will be processed in accordance with current legislation on privacy. Therefore the Company undertakes to process said data in accordance with the principles of fairness, lawfulness and transparency, in compliance with the purposes set out below, collecting said data only for specified and necessary purposes. Only authorised and properly trained personnel will be allowed the use of said data in order to guarantee the necessary confidentiality of the information provided.

Specifically, the Company retains the data necessary exclusively to comply with legal requirements, as well as the protection of the Company's right to defend itself and will consult said data in order to comply with specific legal requirements, or fulfil requests by authorities or in the event of judicial or administrative proceedings.

The Company, through regular checks, will constantly ensure that the data retained are strictly relevant and indispensable and not excessive for the terminated employment relationship, work or position, also in reference to the data provided by the data subject voluntarily.

Specifically, the Company will process your data for the following purposes:

1) comply with legal requirements, particularly with regard to tax-administrative obligations. The lawfulness of processing is based on applicable regulations;

2) respond to requests from Authorities, as well as assert or defend a right in court or in arbitration and conciliation procedures in the cases provided for by law, by European Union law and regulations or collective agreements. The lawfulness of processing is based on the contract between you and the Company.

Retention period of personal data

Your data will be retained in accordance with the following criteria:

- to fulfil legal obligations and for tax-administrative purposes regarding Company operations, the data will be kept for the maximum time allowable by industry regulations;

- to respond to requests from Authorities, as well as assert or defend a right in court or in arbitration and conciliation procedures in the cases provided for by law, by European Union law and regulations or collective agreements, within the terms of your legal rights.

Transfer and access to personal data

The Company - without needing your specific consent - may communicate your personal data to other subjects, the categories of which are described in detail below, for example:

- third parties (for example credit institutes, professional firms, consultants, insurance companies for the provision of insurance services, payroll companies, etc.) who carry out outsourcing activities on behalf of the Data Controller, in their capacity as Data Processors;

- Judicial authorities, insurance companies for the provision of insurance services, as well as those subjects to whom communication is required by law. These subjects will process the data in their capacity as independent Data Controllers.

Your rights

With reference to the data processed, the Company guarantees that you have the right:

- to receive confirmation of the existence of your personal data and to receiving it in an intelligible form.
- to obtain the updating, rectification or integration of your data;
- to request the deletion of your data, within the terms permitted by law, or request the pseudonymisation of your data;
- to object, in whole or in part, for legitimate reasons, to the processing of your personal data;
- to restrict the processing, in case of violation, request for rectification or opposition;
- to request the portability of electronically processed data, provided on the basis of consent or contract;
- to withdraw consent for the processing of your data, if required.

For this purpose, the Company has provided a specific section on the website where you can download the necessary forms. Alternatively, you may request the forms by sending an email to the following address: xxxx to submit your requests free of charge.

Please be informed that the Company shall undertake to respond to your requests within one month, except in cases of particular complexity, so it may take up to 3 months. In any case, the Company will notify you of any delay within one month of your request.

You will receive your reply in writing, either digitally or on hard copy. Should you request the rectification, the cancellation and the limitation of data processing, the Company undertakes to notify each recipient of your data of your request, unless this proves to be impossible or involves a disproportionate effort.

Please remember that the withdrawal of consent, if the lawfulness of processing was based on consent, does not affect the lawfulness of the processing, before revocation of consent.

Please be advised that you may be asked for payment, if your applications are manifestly unfounded, excessive or repetitive; to this end, the Company keeps a register to track your requests for action.

City/Date

1.5 Informativa Privacy per i Visitatori
Data di aggiornamento dell'informativa: xxxx

Gentile Visitatore, prima di procedere al trattamento dei suoi dati, Le sottoponiamo l'informativa Privacy prevista da xxxxx (di seguito semplicemente Società), necessaria per la tutela dei suoi dati personali, secondo quanto previsto dalla normativa in materia.

Le informazioni di seguito riportate le saranno utili per comprendere:
- quali sono i soggetti che trattano i suoi dati e come contattarli;
- come vengono analizzati i suoi dati e per quale motivo.

Contatti utili

xxxxx è la Società che tratta i suoi dati ed ai fini di Legge, è considerata Titolare del trattamento dei dati. In tale veste essa è responsabile di garantire l'applicazione delle misure organizzative e tecniche necessarie e adeguate alla protezione dei suoi dati. La sede della Società è in Via xxxx, xx xxxx xxxx, xxx – xxxx. E-mail: xxxxxx.

Inoltre la Società ha nominato il Responsabile alla Protezione dei Dati (DPO) incaricato di garantire il rispetto delle norme per la tutela della sua Privacy, contattabile per questioni inerenti il trattamento dei suoi dati, al seguente indirizzo di posta elettronica: xxxxxx. Potrà trovare maggiori informazioni sui suoi diritti nello spazio dedicato "I suoi diritti".

Informazioni sul trattamento

Le precisiamo che tutti i dati personali che Lei ci fornirà saranno trattati in conformità alla vigente normativa in materia di privacy, pertanto la Società si impegna a trattarli secondo principi di correttezza, liceità, trasparenza, nel rispetto delle finalità di seguito indicate, raccogliendoli nella misura necessaria ed esatta per il trattamento, consentendone l'utilizzo solo da personale allo scopo autorizzato e formato ed al fine di garantire la necessaria riservatezza delle informazioni fornite.

In particolare, la Società La informa che i suoi dati potranno essere rilevati e registrati con sistemi di videosorveglianza, da utilizzarsi anche quale mezzo di prova ai sensi della normativa vigente, per consentire la gestione del controllo accessi alle sedi e uffici di xxxx e alle relative aree di pertinenza, a fini di sicurezza e tutela delle persone e del patrimonio aziendale, rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo e comunque a qualsiasi azione o evento doloso o colposo che possa arrecare nocumento, attuale o potenziale alle risorse umane ed ai beni materiali ed immateriali dell'azienda, nonché ai fini di prevenzione di incendi o di sicurezza del luogo di lavoro. La base giuridica del trattamento è il legittimo interesse.

Le apparecchiature utilizzate possono essere anche di tipo c.d. "intelligente", cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli ed eventualmente registrarli. Sarà edotto della presenza di sistemi di rilevazione attraverso la visione di apposito segnale, indicato dal Garante alla protezione dei dati personali, di seguito riportato.

Periodo di conservazione dei suoi dati Conformemente a quanto previsto dalla normativa, la conservazione dei dati avverrà per un termine di 7 giorni, de- corsi i quali, i dati verranno cancellati definitivamente.

Possono essere previsti termini maggiori, solo di fronte alla richiesta da parte dell'Autorità giudiziaria o dall'organo delegato in relazione ad attività investigative in corso.

Trasferimento e accesso ai suoi dati

La Società — senza che sia necessario richiedere il suo specifico consenso — può comunicare i suoi dati personali a categorie di soggetti di seguito meglio, quali ad esempio:

- Società del Gruppo, in qualità di responsabili del trattamento, anche non presenti all'interno dell'UE (sulla base delle decisioni di adeguatezza della Commissione Europea o sulla base delle standard model clauses), al fine di svolgere attività di controllo e gestione del personale;

- Autorità giudiziarie.

Non è prevista la comunicazione a terze parti.

I suoi diritti

Con riferimento ai dati trattati, la Società Le garantisce la possibilità di:

- ottenere la conferma dell'esistenza o meno dei dati personali che La riguardano e la loro copia in forma intelligibile;
- ottenere l'aggiornamento, la rettificazione o l'integrazione dei suoi dati;
- richiedere la cancellazione dei suoi dati, nei termini consentiti dalla normativa, oppure chiedere che siano anonimizzati;
- opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano;
- limitare il trattamento, in caso di violazione, richiesta di rettifica od opposizione;
- chiedere la portabilità dei dati trattati elettronicamente, forniti sulla base di consenso o contratto;
- revocare il consenso al trattamento dei suoi dati, qualora previsto.

A tale scopo, la Società ha previsto sul sito internet una specifica sezione in cui può scaricare i moduli. In alternativa La invita a recuperare i moduli inviando una mail al seguente indirizzo: xxxx per presentare le sue richieste in maniera gratuita.

La informiamo che la Società si impegna a rispondere alle sue richieste entro il termine di un mese, salvo caso di particolare complessità, per cui potrebbe impiegare massimo 3 mesi. In ogni caso, la Società provvederà a spiegare il motivo dell'attesa entro un mese dalla sua richiesta.

L'esito della sua richiesta Le verrà fornito per iscritto o su formato elettronico. Nel caso chieda la rettifica, la cancellazione nonché la limitazione del trattamento, la Società si impegna a comunicare gli esiti delle sue richieste a ciascuno dei destinatari dei suoi dati, salvo che ciò risulti impossibile o implichi un o sforzo sproporzionato.

Si ricorda che la revoca del consenso, qualora questa fosse la base giuridica del trattamento, non pregiudica la liceità del trattamento basato sul consenso, prima della revoca.

La Società specifica che Le potrà essere richiesto un eventuale contributo, qualora le sue domande risultino manifestamente infondate, eccessive o ripetitive; a tal proposito, la Società si è dotata di un registro per tracciare le sue richieste di intervento.

Privacy Notice for Visitors

Updated on: xxxx

Dear Visitor, before proceeding with the processing of your data, please read the Privacy notice provided by xxxx (hereinafter “the Company”), necessary for the protection of your personal data, as required by privacy legislation.

The information below will be useful to help you understand:
- who will process your data and how to contact them;
- how your data will be analysed and for what reason.

Useful contacts

xxxx is the Company that processes your data and for the purposes of the law, is the Data Controller. In this capacity it is responsible for ensuring the application of necessary and adequate organisational and technical measures to protect your data. The Company is based in Via xxxx, xxx xxx xxxx, xxx - xxx. E-mail: xxxxx.

Additionally, the Company has appointed a Data Protection Officer (DPO) who will be responsible for ensuring compliance with the rules for protecting your Privacy and who can be contacted for matters concerning personal data processing, at the following e-mail address: xxxx. You can find more information about your rights in the "Your rights" section.

Information on data processing

Please note that all the personal data provided by you will be processed in accordance with current legislation on privacy. Therefore the Company undertakes to process said data in accordance with the principles of fairness, lawfulness and transparency, in compliance with the purposes set out below, collecting said data only for specified and necessary purposes. Only authorised and properly trained personnel will be allowed the use of said data in order to guarantee the necessary confidentiality of the information provided.

Please be informed that your data may be registered or recorded by video surveillance system, which may also be used as evidence pursuant to current regulations, to allow for managing access to xxxx sites and offices and related areas in order to protect compa- ny personnel and assets from attacks, theft, kidnapping, damage, vandalism and, in any case, from any fraudulent or culpable actions or events, capable of causing damage, both actual or potential, to human resources and to the company's material and immaterial assets as well as for fire prevention or workplace safety. The lawfulness of processing is based on legitimate interest;

The equipment used can also be "intelligent", in other words it is able to automatically detect behaviour or anomalous events, to report them and if necessary, to record them. The presence of detection systems is posted on specific signs, as instructed by the Data Protection Authority, as shown below.

Retention period of personal data

In accordance with the provisions of the law, the data will be retained for a period of 7 days, after which, the data will be deleted permanently.

A longer period may be provided for, only in response to a request by the judicial authority or by the delegated body in relation to ongoing investigations.

Transfer and access to your data

The Company - without needing your specific consent - may communicate your personal data to other subjects, the categories of which are described in detail below, for example:

- xxxxx Group companies, in their capacity as data processors, even if not located in the EU (based on the adequacy decisions by the European Commission or on the basis of standard model clauses), in order to carry out personnel management and control activities;

- Judicial authorities.

Data will not be transferred to third parties.

Your rights

With reference to the data processed, the Company guarantees that you have the right:

- to receive confirmation of the existence of your personal data and to receiving it in an intelligible form.
- to obtain the updating, rectification or integration of your data;
- to request the deletion of your data, within the terms permitted by law, or request the pseudonymisation of your data;
- to object, in whole or in part, for legitimate reasons, to the processing of your personal data;
- to restrict the processing, in case of violation, request for rectification or opposition;
- to request the portability of electronically processed data, provided on the basis of consent or contract;
- to withdraw consent for the processing of your data, if required.

For this purpose, the Company has provided a specific section on the website where you can download the necessary forms. Alternatively, you may request the forms by sending an email to the following address: xxxxx to submit your requests free of charge.

Please be informed that the Company shall undertake to respond to your requests within one month, except in cases of particular complexity, so it may take up to 3 months. In any case, the Company will notify you of any delay within one month of your request.

You will receive your reply in writing or digitally. Should you request the rectification, the cancellation and the limitation of data processing, the Company undertakes to notify each recipient of your data of your request, unless this proves to be impossible or involves a disproportionate effort.

Please remember that the withdrawal of consent, if the lawfulness of processing was based on consent, does not affect the lawfulness of the processing, before revocation of consent.

Please be advised that you may be asked for payment, if your applications are manifestly unfounded, excessive or repetitive; to this end, the Company keeps a register to track your requests for action.

1.6 INFORMATIVA DA UTILIZZARE CON TERZE PARTI - PERSONE GIURIDICHE

1) NUOVA PRIVACY

Informativa sul Regolamento europeo 2016/679 del 27 aprile 2016 per il trattamento dei dati forniti

Nel corso dello svolgimento di tutte le attività connesse all'esecuzione del presente contratto, ciascuna delle parti potrà trovarsi nella condizione di dover trattare dati personali riferibili a dipendenti e/o collaboratori dell'altra parte, motivo per il quale ciascuna di esse s'impegna sin d'ora a procedere al trattamento di tali dati personali in conformità alle disposizioni di cui al Regolamento Europeo EU 679/2016 in materia di protezione dei dati personali, nonché tutte le norme di legge di volta in volta applicabili.

Le parti s'impegnano a condurre le attività di trattamento di dati personali sulla base dei principi di correttezza, liceità, trasparenza e tutela della riservatezza dei soggetti interessati e per il solo ed esclusivo fine di perseguire le finalità di cui al presente contratto nonché degli eventuali obblighi di legge allo stesso connessi. I dati personali raccolti nell'ambito del presente contratto saranno trattati da ciascuna delle parti limitatamente al periodo di tempo necessario al perseguimento delle finalità di cui sopra. Nel caso in cui tali dati costituiscano contatti professionali (da intendersi per tali tutti i contatti di professionisti e/o soggetti che agiscono nella loro qualifica professionale), potranno essere trattati sin quando ciascuna delle parti lo ritenga utile al fine di dar corso ad una possibile prosecuzione della collaborazione professionale. A tal proposito, ciascuna delle parti si impegna a render accessibili detti dati solo ai propri dipendenti e/o collaboratori che, in ragione della propria funzione e/o attività, hanno la necessità di trattare gli stessi, per il fine di cui sopra. Le parti dichiarano espressamente di aver debitamente informato e di informare i propri dipendenti e/o collaboratori man mano che diverrà necessario.

(parte da valutare di volta in volta)

Qualora, nell'ambito di svolgimento delle prestazioni di cui al presente contratto, ciascuna delle parti si trovi nella condizione di affidare in parte e/o in toto attività di trattamento di dati personali di propria titolarità e/o per i quali sia stata nominata responsabile del trattamento da altro titolare, entrambe s'impegnano a sottoscrivere un separato accordo scritto volto a formalizzare la nomina a responsabile e/o sub-responsabile del trattamento della parte affidataria al fine di procedere ad una corretta gestione delle attività di trattamento di dati personali così come previsto dall'articolo 28 Regolamento Europeo EU

679/2016. La sottoscrizione di tale accordo, qualora sussistano le esigenze di cui sopra, è condizione necessaria ed imprescindibile per l'affidamento di attività di trattamento di dati personali.

2) NUOVA PRIVACY – Clausola in INGLESE

Information as per Regulation (EU) n. 679/2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data.

Each of the parties, by carrying out all the activities in connection with the execution of the present contract, may find itself in the position of having to process personal data related to employees and/or collaborators of the other party, which is why each party undertakes, as of now, to treat such personal data in accordance with the provisions of the European Regulation EU 679/2016 on the protection of personal data, as well as any other legal provisions which may be applicable from time to time.

The parties undertake to process personal data in accordance with the principles of correctness, lawfulness, transparency and protection of privacy of the parties to whom the data relate, for purposes strictly connected with the performance of this contract and the fulfillment of all related legal obligations. Personal data acquired by the parties in execution and/or on the occasion of this contract will be processed by each party for the period of time necessary to achieve the aforementioned purposes. Should such data constitute business contacts, they can be processed as long as each of the parties deems appropriate in view of a possible continuation of the business relationship. In this regard, each of the parties undertakes to limit access to the data only to those of its employees and/or collaborators who need access for the purposes described above. The parties expressly declare to have duly informed and to inform their respective employees and/or collaborators as it becomes necessary.

(to be evaluated from time to time)

Where, in the performance of the services under this contract, each of the parties requires to entrust in whole and/or in part the activities concerning the processing of personal data for which each party is responsible, both parties undertake to enter into a separate written agreement providing for the appointment of a data protection officer and/or other officers of the entrusted party to ensure that the processing of personal data meets the requirements of Article 28 of the Regulation EU679/2016. The agreement, if the above requirements exist, is a necessary and unavoidable condition to entrust personal data processing activities.

1. 7 INFORMATIVA DA UTILIZZARE CON TERZE PARTI - PERSONE FISICHE

3) NUOVA PRIVACY

Informativa ex Art. 13 del D.Leg. n. 196/2003 e ex Art. 13 del Regolamento europeo 679/2016 per il trattamento dei dati forniti

Lei riconosce, anche ai sensi e per gli effetti degli art. 13 del D. Leg. 196/2003 e dell'art. 13 del Regolamento europeo 2016/679, che i dati personali acquisiti in esecuzione e/o in occasione del presente accordo potranno essere da noi trattati, con o senza l'ausilio di mezzi elettronici, per le finalità connesse allo svolgimento della nostra attività economica, ed in tali limiti possono essere comunicati a terzi. La prevalenza dei trattamenti di cui sopra risponde ad obblighi contrattuali, contabili e fiscali ed in tali limiti il conferimento deve ritenersi necessario. Il trattamento dei dati personali si basa sul rapporto contrattuale instaurato e dovrà intendersi autorizzato per l'intera durata del contratto e per l'ulteriore periodo di tempo necessario per rispondere agli obblighi di legge. Noi adotteremo misure contrattuali, tecniche e organizzative appropriate al fine di garantire la conformità con le leggi sulla privacy applicabili anche con riferimento al trasferimento e al trattamento dei dati personali al di fuori dell'Unione Europea. Lei potrà esercitare i diritti di cui all'art. 7 del D. Leg. 196/2003 e agli artt. 15 e seguenti del Regolamento EU n. 679/2016 che dichiara di ben conoscere. Titolare dei trattamenti di cui sopra è la Società XXX. DPO della Società XXX è il Signor _____ (email: _____).

4) NUOVA PRIVACY – Clausola in INGLESE

Information as per art. 13 of the Italian Government Decree 196/2003 and art. 13 of the Regulation (EU) n. 679/2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

As per art. 13 of Italian Government Decree 196/2003 and art. 13 of the Regulation (EU) 679/2016, you acknowledge that your personal data acquired by **XXX** in execution and/or on the occasion of this agreement will be treated, with or without use of electronic means, for purposes strictly connected with the performance of its commercial activity, and, subject to such restrictions, they may be disclosed to third parties. The use of the above data mainly derives from contractual, accounting and fiscal obligations and, subject to such restrictions, the disclosure of the data must be considered as necessary. The processing of personal data is based on the established contractual relationship between you and **XXX**

and must be regarded as authorized for the entire term of the contract and for the additional period of time required to meet legal obligations. **XXX** will take appropriate contractual, technical and organizational measures to ensure compliance with applicable privacy rules or regulations also with regard to the movement and processing of personal data outside the European Union. You may exercise your rights as per art. 7 of Decree 196/2003 and artt. 15 and subsequent of Regulation (EU) 679/2016, contents of which you declare to know. **XXX** is responsible of the data treatment. **XXX** DPO is _____ (e-mail:_____).

2. I DIRITTI DEGLI INTERESSATI: DISAMINA, RACCOMANDAZIONI E ALERT

Diritti degli interessati

DIRITTO DI ACCESSO

DIRITTO DI RETTIFICA

DIRITTO ALL'OBLIO

DIRITTO DI LIMITAZIONE

DIRITTO ALLA PORTABILITÀ

DIRITTO DI OPPOSIZIONE

Introduzione

Il Regolamento assegna all'interessato i suoi diritti, in particolare essi vengono dapprima descritti genericamente all'interno dei considerando dal 58 al 73 (che sono una sorta di "premesse" al Regolamento), e poi elencati e definiti negli articoli dal 12 al 23.

Ma quali sono quindi questi diritti? Il Regolamento assegna all'interessato del trattamento, salvo le eccezioni stabilite all'art. 23, i seguenti diritti:

- Accesso;
- Rettifica;
- Oblio;
- Limitazione del Trattamento;
- Portabilità dei dati;
- Opposizione al Trattamento.

Nel seguito si allega una piccola analisi diritto per diritto con una serie di raccomandazioni ed alert.

Limitazioni art. 23 GDPR

Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;

f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;

g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;

h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);

i) la tutela dell'interessato o dei diritti e delle libertà altrui;

j) l'esecuzione delle azioni civili.

2. In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso:

a) le finalità del trattamento o le categorie di trattamento;

b) le categorie di dati personali;

c) la portata delle limitazioni introdotte;

d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;

e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;

f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;

g) i rischi per i diritti e le libertà degli interessati; e

h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

Diritto di accesso

	ARTICOLO	OBBLIGHI TITOLARE	OBBLIGHI RESPONSABILE	TEMPI	RACCOMANDAZIONI	MODALITA'
DIRITTO DI ACCESSO	15	Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura, sia tecnica che organizzativa, a ciò idonea. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.	il responsabile è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti degli interessati	1 mese, estensibile fino a 3 mesi nelle ipotesi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego	Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento. Tra le informazioni che il titolare deve fornire non rientrano le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione previsto ovvero, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi	Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, e può essere dato oralmente solo se così richiede l'interessato stesso. La risposta fornita dall'interessato. Deve essere concisa, trasparente e facilmente accessibile, deve utilizzare un linguaggio semplice e chiaro.

Diritto di rettifica

	ARTICOLO	OBBLIGHI TITOLARE	OBBLIGHI RESPONSABILE	TEMPI	RACCOMANDAZIONI	MODALITA'
DIRITTO DI RETTIFICA	16	Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura, sia tecnica che organizzativa, a ciò idonea. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.	il responsabile è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti degli interessati	1 mese, estensibile fino a 3 mesi nelle ipotesi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego	l'interessato avrà la possibilità di ottenere dal titolare del trattamento la correzione senza ritardo dei dati inesatti che lo riguardano. Inoltre, tenuto conto delle finalità del trattamento, l'interessato potrà ottenere l'integrazione dei propri dati incompleti, anche fornendo una dichiarazione integrativa.	Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, e può essere dato oralmente solo se così richiede l'interessato stesso. La risposta fornita dall'interessato. Deve essere concisa, trasparente e facilmente accessibile, deve utilizzare un linguaggio semplice e chiaro.

Diritto all’oblio

	ARTICOLO	OBBLIGHI TITOLARE	OBBLIGHI RESPONSABILE	TEMPI	RACCOMANDAZIONI	MODALITA'
DIRITTO ALL'OBLIO	17	Il titolare del trattamento deve agevolare l’esercizio dei diritti da parte dell’interessato, adottando ogni misura, sia tecnica che organizzativa, a ciò idonea. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l’interessato, e quest’ultimo ha il dovere di fornirle, secondo modalità idonee.	il responsabile è tenuto a collaborare col titolare ai fini dell’esercizio dei diritti degli interessati	1 mese, estensibile fino a 3 mesi nelle ipotesi di particolare complessità. Il titolare deve comunque dare un riscontro all’interessato entro 1 mese dalla richiesta, anche in caso di diniego	Il diritto “all’oblio” si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l’obbligo per i titolari (se hanno “reso pubblici” i dati personali dell’interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi “qualsiasi link, copia o riproduzione”. Risulta più esteso di quello già riconosciuto all’art. 7, comma III, lettera b), del Codice della privacy, poiché l’interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento.	Il riscontro all’interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l’accessibilità, e può essere dato oralmente solo se così richiede l’interessato stesso. La risposta fornita dall’interessato. Deve essere concisa, trasparente e facilmente accessibile, deve utilizzare un linguaggio semplice e chiaro.

Diritto di limitazione

	ARTICOLO	OBBLIGHI TITOLARE	OBBLIGHI RESPONSABILE	TEMPI	RACCOMANDAZIONI	MODALITA'
DIRITTO DI LIMITAZIONE	18	Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura, sia tecnica che organizzativa, a ciò idonea. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.	il responsabile è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti degli interessati	1 mese, estensibile fino a 3 mesi nelle ipotesi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego	Rappresenta un diritto differente e maggiormente esteso rispetto al "blocco" del trattamento già previsto dall'art. 7, comma III, lettera a), del Codice della Privacy. In particolare risulta esercitabile non solamente in ipotesi di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì pure se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del Regolamento (in attesa della valutazione da parte del titolare). Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).	Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, e può essere dato oralmente solo se così richiede l'interessato stesso. La risposta fornita dall'interessato. Deve essere concisa, trasparente e facilmente accessibile, deve utilizzare un linguaggio semplice e chiaro.

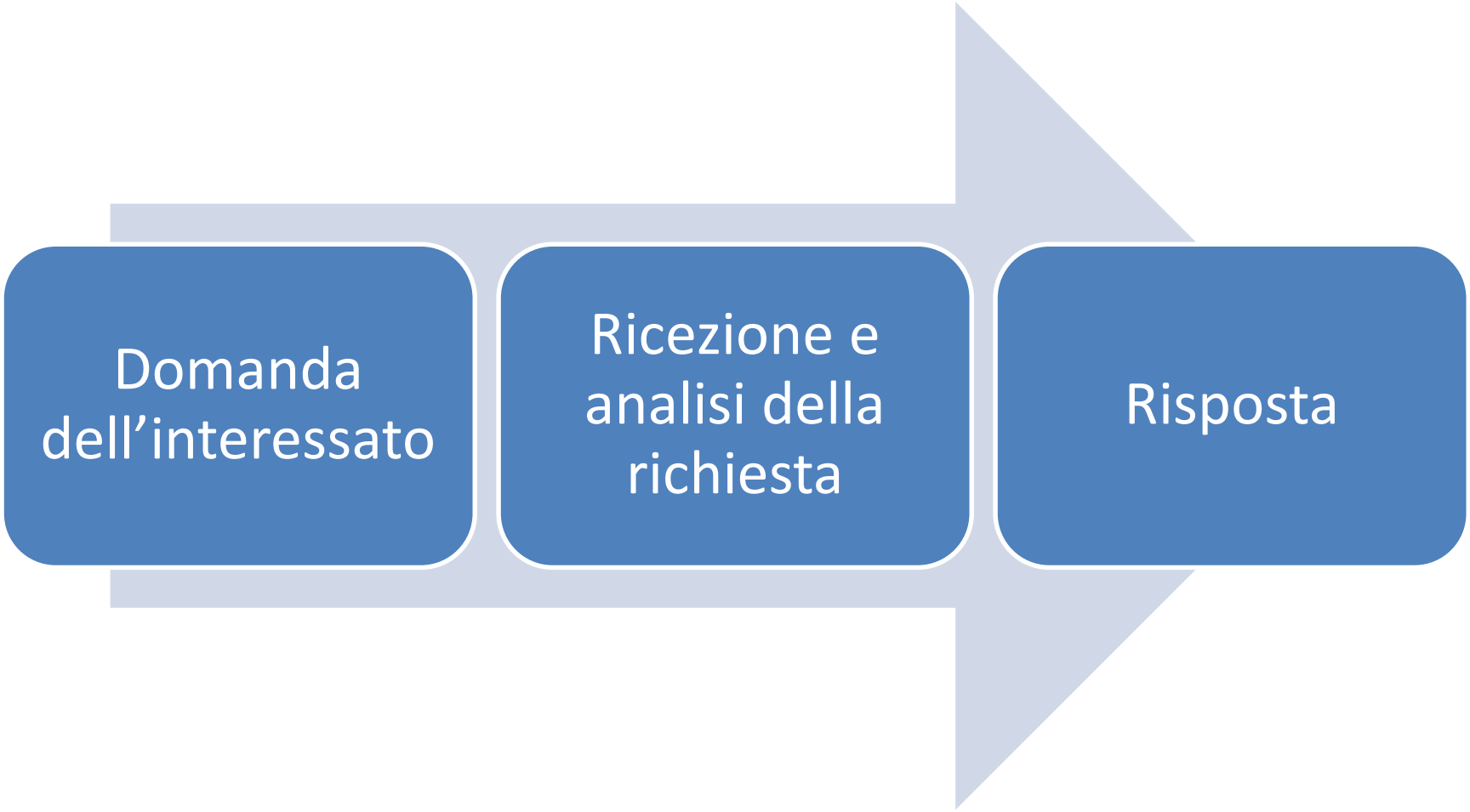
Diritto alla portabilità

	ARTICOLO	OBBLIGHI TITOLARE	OBBLIGHI RESPONSABILE	TEMPI	RACCOMANDAZIONI	MODALITA'
DIRITTO ALLA PORTABILITA'	20	Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura, sia tecnica che organizzativa, a ciò idonea. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.	il responsabile è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti degli interessati	1 mese, estensibile fino a 3 mesi nelle ipotesi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego	Rappresenta un diritto "nuovo" previsto dal Regolamento, pure se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico). Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio. In particolare risultano portabili soltanto i dati trattati col consenso dell'interessato ovvero sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare), e solo i dati che siano stati "forniti" dall'interessato al titolare. Il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, qualora tecnicamente possibile.	Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, e può essere dato oralmente solo se così richiede l'interessato stesso. La risposta fornita dall'interessato. Deve essere concisa, trasparente e facilmente accessibile, deve utilizzare un linguaggio semplice e chiaro.

Diritto di opposizione

	ARTICOLO	OBBLIGHI TITOLARE	OBBLIGHI RESPONSABILE	TEMPI	RACCOMANDAZIONI	MODALITA'
DIRITTO DI OPPOSIZIONE	21	Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura, sia tecnica che organizzativa, a ciò idonea. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.	il responsabile è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti degli interessati	1 mese, estensibile fino a 3 mesi nelle ipotesi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego	L'esercizio di tale diritto rappresenta l'obbligo, in capo al titolare, di astenersi dal trattamento dei dati. Questo particolare diritto riguarda però situazioni in cui il titolare sta lecitamente trattando dei dati personali: pertanto, è riconosciuta la facoltà per il titolare di dimostrare che i suoi interessi specifici connessi al trattamento prevalgono su quelli evidenziati dall'interessato.	Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, e può essere dato oralmente solo se così richiede l'interessato stesso. La risposta fornita dall'interessato. Deve essere concisa, trasparente e facilmente accessibile, deve utilizzare un linguaggio semplice e chiaro.

Esercizio dei diritti



Procedura in caso di esercizio dei diritti da parte dell'interessato 1/7

Al fine di meglio gestire i diritti degli interessati, è opportuno che ogni società definisca un'apposita procedura da attivare in caso di richiesta di esercizio dei diritti da parte degli interessati.

Nel seguito si forniscono alcuni spunti per la sua predisposizione:

1 – arrivo della domanda dell'interessato

E' necessario che la richiesta pervenuta sia portata immediatamente all'attenzione dell'ufficio che si occupa di privacy e se nominato del DPO.

2 – gestione della richiesta considerando la tempistica ristretta di un mese (estendibile fino a 3 per casi di particolare complessità)

L'ufficio privacy dovrà analizzare la richiesta e procedere al coinvolgimento delle varie funzioni coinvolte a seconda del tipo di diritto che l'interessato vuol far valere (es: funzione IT, marketing ecc.), coinvolgendo il Responsabile di riferimento.

Sulla base delle mappature dei trattamenti dei dati della società inserite nel registro, l'ufficio privacy o il soggetto identificato all'analisi dovrà identificare i processi aziendali che sono coinvolti dalla richiesta.

Dato che come titolare si potrebbero trattare anche una notevole quantità di informazioni dello stesso interessato (ad esempio perché i dati sono trattati per numerose finalità distinte, infatti l'interessato potrebbe essere, un dipendente, un ex dipendente, un cliente, un fornitore ecc. o potrebbe ricoprire contemporaneamente più posizioni), se la richiesta dell'interessato è generica e con consente di identificare esattamente l'ambito nel quale concentrare l'analisi, sarà necessario chiedere subito delle precisazioni all'interessato, per cercare di circoscrivere quanto possibile l'ambito della richiesta.

3 – risposta

Il riscontro all'interessato deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, e può essere dato oralmente solo se così richiede l'interessato stesso.

La risposta deve essere concisa, trasparente e facilmente accessibile, deve utilizzare un linguaggio semplice e chiaro.

Le informazioni dovranno essere date a titolo gratuito.

Se la risposta ha determinato una spesa tecnica rilevante (ad esempio, qualora siano state richieste più copie) oppure le richieste dell'interessato siano risultate infondate o eccessive: si potrà quindi addebitare entro limiti ragionevoli all'interessato una parte delle spese e richiedergli il versamento di un contributo.

Procedura in caso di esercizio dei diritti da parte dell'interessato 2/7

3. 1 – contenuto della risposta in caso di diritto di accesso

Ricevuta la richiesta l'Ufficio privacy si attiverà e fornirà all'interessato la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e fornirà all'interessato - con gli accorgimenti necessari volti ad evitare la lesione di diritti e di libertà altrui - una copia dei dati personali oggetto di trattamento, oltre alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- il periodo di conservazione dei dati personali previsto, oppure, se non e possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 GDPR.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'art. 46 GDPR relative al trasferimento.

Procedura in caso di esercizio dei diritti da parte dell'interessato 3/7

3.2 – contenuto della risposta in caso di diritto di rettifica

Ricevuta la richiesta l'Ufficio privacy provvederà alla rettifica dei dati personali dell'interessato, dandone comunicazione all'interessato.

In caso di richiesta di integrazione dei dati personali da parte dell'interessato, si dovrà valutare, in via preliminare, se l'integrazione richiesta possa violare il principio di "limitazione della finalità" e/ o di "minimizzazione dei dati" stabiliti dall'art. 5 del GDPR.

Nel caso in cui vi sia violazione di uno dei due principi sopra richiamati, non si potrà ottemperare alla richiesta di integrazione dei dati personali dandone motivato riscontro all'interessato. In caso contrario si provvederà ad integrare i dati, in conformità con la dichiarazione ricevuta dall'interessato.

Procedura in caso di esercizio dei diritti da parte dell'interessato 4/7

3.3 – contenuto della risposta in caso di diritto all'oblio

Ricevuta la richiesta di cancellazione l'Ufficio privacy, previa valutazione della sussistenza dei motivi per ottenere la cancellazione, provvederà alla cancellazione dei dati personali che riguardano l'interessato dandone comunicazione all'interessato.

Nel caso in cui si fossero resi pubblici i dati personali che riguardano un interessato che abbia fatto richiesta di cancellazione e sia stata verificata l'effettiva sussistenza del diritto alla cancellazione dei dati in capo al richiedente, si adotteranno misure ragionevoli, anche tecniche (tenendo conto della tecnologia disponibile e dei costi di attuazione) per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Si provvederà inoltre a comunicare a ciascuno dei destinatari cui, eventualmente, sono stati trasmessi i dati personali oggetto di cancellazione le cancellazioni effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. II titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Nel caso in cui non si ritengano sussistenti i motivi per ottenere la cancellazione si provvederà a comunicarlo all'interessato, tenendo conto che il diritto di ottenere la cancellazione non spetta all'interessato nella misura in cui il trattamento sia necessario:

- per l' esercizio del diritto alla liberta di espressione e di formazione;
- per l'adempimento di un obbligo legale o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui e investito il titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici nella misura in cui il diritto alla cancellazione dei dati personali rischia di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Procedura in caso di esercizio dei diritti da parte dell’interessato 5/7

3.4 – contenuto della risposta in caso di diritto di limitazione

Ricevuta la richiesta di limitazione l’Ufficio Privacy, previa valutazione della sussistenza dei presupposti di fatto per ottenere la limitazione, provvederà a limitare il trattamento dei dati personali dell'interessato che ne ha fatto richiesta, dandone comunicazione all'interessato.

I dati personali il cui trattamento viene limitato dovranno essere contrassegnati in attesa di determinazioni ulteriori e dovranno essere trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico.

Si provvederà a comunicare a ciascuno dei destinatari cui, eventualmente, sono stati trasmessi i dati personali oggetto di limitazione del trattamento le limitazioni effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

In caso di revoca della limitazione al trattamento, si provvederà ad informare l'interessato.

Procedura in caso di esercizio dei diritti da parte dell’interessato 6/7

3.5 – contenuto della risposta in caso di diritto alla portabilità

Le modalità di esercizio del diritto alla portabilità dei dati saranno dettagliatamente comunicate all'interessato al momento della richiesta.

Le modalità di esercizio del diritto varieranno a seconda del contenuto e della valutazione di fattibilità della richiesta formulata dall'interessato.

Il diritto alla portabilità dei dati non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi e registri cartacei), si precisa che sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato. I dati per cui può essere richiesta la portabilità sono solo quelli forniti dall'interessato al titolare del trattamento.

L'esercizio del diritto alla portabilità dei dati, oltre a non dover ledere i diritti e le liberta altrui, non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare.

Procedura in caso di esercizio dei diritti da parte dell'interessato 7/7

3.6 – contenuto della risposta in caso di diritto di opposizione

Ricevuta l'opposizione e valutati i motivi su cui si fonda l'opposizione, l'Ufficio privacy dovrà far sì che ci si astenga dal trattare ulteriormente i dati personali salvo che ci siano motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle liberta dell'interessato oppure per l'accertamento, l'esercizio e la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Ricevuta l'opposizione al trattamento per finalità di marketing diretto, non si potrà più trattare i dati personali per tali finalità.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma

dell'art. 89, paragrafo 1, GDPR, l'interessato, per motivi connessi alla sua situazione particolare, ha

il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

3. TITOLARE E RESPONSABILE DEL TRATTAMENTO

3.1 Data Protection Addendum

I

Atto di nomina di responsabile esterno al trattamento dei dati

I. Scopo del presente atto

Con il presente atto il Sig. …… in qualità di ……. presso la Società ……. in quanto Appaltatore ai sensi del contratto n. ……. di cui il presente atto è allegato viene nominato Responsabile esterno al trattamento dei dati e in quanto tale, si impegna a svolgere secondo le istruzioni impartire dal Committente, xxxxxxx di seguito Titolare, con sede in Via xxxxx, xx, xxxxx xxxx, xxxx - xxxxx e per conto di quest'ultimo, le operazioni di trattamento dei dati personali definite di seguito.

Il dottore …… nomina l'Appaltatore in vista dei poteri ricevuti.

Nell'ambito delle loro relazioni contrattuali, le parti si impegnano a rispettare la riservatezza dei dati di seguito indicati nonché le norme in vigore applicabili al trattamento dei dati personali previste dal D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 applicabile a decorrere dal 25 maggio 2018 (di seguito: GDPR).

II. Descrizione del trattamento concesso all'Appaltatore, ex art. 28 del GDPR

L'Appaltatore è autorizzato a trattare secondo le istruzioni fornite dal Titolare del trattamento e per conto di quest'ultimo, i dati personali necessari per fornire i servizi sottesi al contratto di cui il presente è allegato.

In particolare, l'Appaltatore tratterà in maniera automatizzata e non i dati personali comuni/particolari/giudiziari, secondo quanto previsto dalla normativa sopra indicata, degli interessati quali i dipendenti/ex dipendenti/candidati/fornitori per la finalità prevista dal contratto e per la durata del tempo prevista dallo stesso.

Qualora l'Appaltatore tratti i dati acquisiti per finalità diverse, esso è considerato Titolare autonomo e in quanto tale risponde delle eventuali violazioni

III. Durata del contratto

Si fa riferimento al contratto di cui il presente documento è un allegato.

IV. Obblighi dell'Appaltatore nei confronti del Titolare del trattamento

L'Appaltatore nel trattamento dei dati si impegna a rispettare quanto indicato di seguito e dalle istruzioni impartite dal Titolare.

Qualora l'Appaltatore ritenga che un'istruzione costituisca una violazione di legge o del Regolamento europeo della protezione dei dati o di qualsiasi altra disposizione del diritto dell'Unione o della

legislazione degli Stati membri relativa alla protezione dei dati, ne informa immediatamente il Titolare del trattamento. Eventuali deroghe dall'applicazione delle misure tecniche impartite devono essere espressamente autorizzate dal Titolare.

Inoltre, qualora l'Appaltatore sia tenuto a trasferire dati a un paese terzo o ad un'organizzazione internazionale a norma del diritto dell'Unione o della legislazione dello Stato membro cui è soggetto, è tenuto ad informare il Titolare del trattamento prima del trasferimento dei dati oggetto e indicare quali misure di garanzia ha adottato tra quelle previste GDPR, in particolare:

- la conformità a quanto indicato alle decisioni di adeguatezza, secondo quanto indicato dall'art. 45 del GDPR;
- l'adozione di Standard Contractual Clauses previste dalla Commissione europea, secondo art. 46 GDPR. In tal caso, xxxxx autorizza il Fornitore a sottoscrivere in nome proprio e per conto di xxxx le Standard Contractual Clauses previste dal Contratto, con l'impegno del Fornitore a dare evidenza della sottoscrizione e dell'accettazione delle medesime;
- la sottoscrizione di norme vincolanti di impresa, secondo art. 47 GDPR.

1. Formazione del personale autorizzato

L'Appaltatore, in conformità dell'art. 26 del GDPR, deve assicurare che le persone autorizzate al trattamento dei dati personali previsti nel contratto:

- si impegnino a rispettare gli obblighi legali in materia di riservatezza;
- abbiano ricevuto o ricevano adeguata formazione in materia di protezione dei dati personali.

2. Documentazione che l'Appaltatore mette a disposizione del Titolare

Secondo quanto previsto dall'art. 28 del GDPR, l'Appaltatore deve mettere a disposizione del Titolare del trattamento la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi e deve permettere l'esecuzione di ispezioni, svolte sia da parte del Titolare o da soggetto terzo nominato dallo stesso ad eseguire i relativi audit. L'esecuzione delle ispezioni verrà notificata all'Appaltatore almeno ____ giorni prima dell'avvio.

In ogni caso, l'Appaltatore deve dimostrare di aver adottato le policy necessarie per la protezione dei dati e deve procedere con l'esecuzione autonoma di regolari audit indipendenti al fine di garantire il rispetto ai requisiti normativi in materia di privacy e alle policy adottate. Gli esiti dei controlli devono essere a disposizione del Titolare.

Gli audit devono comprendere almeno i seguenti ambiti (per l'elenco completo degli ambiti di controllo richiesti dal Titolare del trattamento si rimanda all'allegato "Specifica Tecnica 1 - Elenco dei controlli – ST 1".):

- tutela della riservatezza, non divulgazione, sicurezza;

- analisi dei rischi in materia di Privacy, secondo quanto previsto dalla normativa indicata;
- ripristino delle attività in caso di emergenza, nonché piani di business continuity e disaster recovery;
- attività degli amministratori di sistema, con elenco aggiornato delle nomine effettuate comprendente le indicazioni sulle funzioni loro attribuite.

Qualora l'Appaltatore sia in possesso di particolari certificazioni deve mettere a disposizione del Titolare la documentazione necessaria e garantire il mantenimento delle stesse per tutta la durata del rapporto. Qualora sopraggiunga qualsiasi ipotesi per cui l'Appaltatore durante l'esecuzione del rapporto, perda la certificazione, deve avvisare prontamente il Titolare e presentare il piano che rappresenta le debolezze sopraggiunte e il piano di ripristino previsto.

La perdita dei requisiti previsti può essere causa di rescissione del rapporto.

3. Privacy by design e by default

L'Appaltatore deve prendere in considerazione, in relazione ai propri strumenti, prodotti, applicazioni o servizi, i principi di protezione dei dati fin dalla fase di progettazione durante la stessa (cfr. art. 25 del GDPR).

4. Nomina di Subappaltatore da parte dell'Appaltatore

Fatto salvo quanto previsto contrattualmente in relazione alla necessaria preventiva autorizzazione al Subappalto, l'Appaltatore può richiedere ad un altro soggetto (in seguito denominato "Subappaltatore") di svolgere attività specifiche di trattamento dei dati.

In tal caso, secondo quanto previsto dall'art. 28 del GDPR, l'Appaltatore deve informare il Titolare di aver nominato per iscritto il Subappaltatore quale responsabile esterno del trattamento, fornendogli le informazioni che indichino chiaramente le attività di trattamento che dovranno essere svolte dal Subappaltatore, l'identità e le informazioni di contatto del Subappaltatore nonché la durata del relativo contratto. Il Titolare, dalla data di ricezione di tali informazioni, ha 30 giorni per presentare le sue obiezioni concernenti le informazioni trasmessegli dall'Appaltatore in ordine al contenuto della nomina a Responsabile esterno del trattamento al Subappaltatore.

L'Appaltatore mette a disposizione del Titolare la lista aggiornata dei Subappaltatori relativi al trattamento dei dati sottesi al contratto di cui il presente atto costituisce allegato.

L'Appaltatore deve fornire al Subappaltatore le istruzioni impartite dal Titolare nel presente atto. Il Subappaltatore è tenuto a rispettare gli obblighi del presente contratto ed a trattare i dati secondo le istruzioni impartite dal Titolare all'Appaltatore.

L'Appaltatore è responsabile di garantire che il Subappaltatore abbia idonee e sufficienti garanzie in merito all'attuazione di misure tecniche e organizzative conformi a quanto richiesto dalla normativa.

A tal proposito l'Appaltatore deve effettuare delle verifiche sull'attività del Subappaltatore nonché garantire l'accesso alla relativa documentazione prodotta al Titolare.

Se il Subappaltatore non rispetta i suoi obblighi in merito al corretto trattamento dei dati, l'Appaltatore rimane pienamente responsabile nei confronti del Titolare.

5. Obbligo di collaborazione in merito ai diritti degli interessati

L'Appaltatore, in conformità dell'art. 28 GDPR, è tenuto a collaborare e supportare il Titolare del trattamento per quanto concerne dell'obbligo di adempiere alle richieste di esercizio dei diritti dei soggetti interessati. Il Titolare è responsabile di fornire le informazioni previste per la tutela dei dati, alle persone interessate dalle attività di trattamento al momento della raccolta dei dati e di mettere a disposizione degli interessati la lista aggiornata dei Responsabili esterni al trattamento dei dati.

6. Notifica di violazioni dei dati personali

L'Appaltatore, in conformità con le disposizioni dell'art. 33 GDPR, comunica al Titolare del trattamento ogni incidente e/o violazione dei dati personali senza ingiustificato ritardo ed entro 48 ore dall'avvenuta conoscenza della violazione, con i mezzi seguenti [indicare indirizzo previsto per la ricezione dei data breach].

Tale notifica è accompagnata da ogni documentazione pertinente affinché il Titolare, se necessario, informi l'Autorità di vigilanza competente dell'infrazione.

La notifica deve contenere almeno:

- una descrizione della natura della violazione di dati personali tra cui, se possibile, le categorie e il numero approssimativo di persone colpite dalla violazione e le categorie e il numero approssimativo di record di dati personali in questione;
- il nome del responsabile della protezione dati o altro punto di contatto dal quale possono essere ottenute ulteriori informazioni;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure che intende adottare per porre rimedio alla violazione dei dati personali, tra cui, se del caso, misure destinate ad attenuare le possibili conseguenze negative.

Se, e nella misura in cui non sia possibile fornire simultaneamente tutte queste informazioni, le informazioni possono essere comunicate in un momento successivo, senza ritardo ingiustificato.

7. Assistenza dell'Appaltatore nel rispetto degli obblighi da parte del Titolare del trattamento

L'Appaltatore assiste il Titolare del trattamento dei dati nell'esecuzione delle valutazioni d'impatto sulla protezione dei dati e se necessaria, nell'esecuzione della consultazione preventiva dell'autorità di vigilanza, in conformità con gli artt. 35 e 36 GDPR.

8. Misure di sicurezza

L'Appaltatore si impegna ad attuare le misure di sicurezza individuate in allegato al presente atto (Cfr. Allegato – "Specifica Tecnica 2 - Misure di sicurezza – ST 2").

Il mancato rispetto delle misure individuate può essere causa di risoluzione del rapporto.

9. Misure di trattamento dei dati dopo la cessazione dei servizi

Come da istruzioni e da indicazioni riportate nell'art. 28 GDPR, l'Appaltatore si impegna a distruggere tutti i dati personali trattati oppure trasferirli al Titolare, salvo l'ipotesi in cui l'Appaltatore sia tenuto a conservare le informazioni raccolte per tutela di interessi legittimi (es. esercizio o difesa di un diritto in sede giudiziaria). Nel caso di cancellazione, l'Appaltatore deve notificare la distruzione di tutte le copie nei sistemi informativi a disposizione. Nel caso in cui i dati vengano conservati, l'Appaltatore deve indicare i motivi e i criteri di conservazione dei dati.

10. Tenuta del registro delle attività di trattamento

L'Appaltatore deve tenere per iscritto il registro delle attività di trattamento dei dati, almeno per i trattamenti svolti per conto del Titolare, contenente le informazioni richieste ed indicate dall'art. 30 GDPR. In particolare l'Appaltatore è tenuto a conservare le seguenti informazioni:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

V. Obblighi del Titolare nei confronti dell'Appaltatore

Il Titolare del trattamento si impegna a:

1. documentare per iscritto tutte le istruzioni relative al trattamento dei dati da fornire all'Appaltatore;
2. assicurare, in anticipo e per tutta la durata del trattamento, il rispetto degli obblighi previsti dalla normativa sulla protezione dei dati da parte di altri Appaltatori nominati;

3. vigilare sui trattamenti dei dati, compresa la conduzione di audit e ispezioni nei confronti dell'Appaltatore.

VI. Responsabilità dell'Appaltatore

Secondo quanto previsto dalla normativa, qualora il Titolari del trattamento e l'Appaltatore siano coinvolti nello stesso trattamento e siano considerati responsabili dell'eventuale danno causato agli interessati, ognuna delle parti è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato. Qualora il Titolare del trattamento o l'Appaltatore, in qualità di Responsabile Esterno del trattamento, abbia pagato l'intero risarcimento del danno, tale parte ha il diritto di reclamare dall'altra parte coinvolta nel trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni previste dalla normativa. Per eventuali trattamenti effettuati dall'Appaltatore in ambiti e per finalità ulteriori e non espressamente richiamati dal presente atto, esso è considerato Titolare autonomo e in quanto tale risponde delle eventuali violazioni.

VII. Allegati "Specifiche Tecniche"

- Specifica Tecnica 1 - Elenco dei controlli – "ST 1";
- Specifica Tecnica 2 - Misure di sicurezza – "ST 2".

Specifica Tecnica 1 - Elenco dei controlli

ID	Requisiti	Possesso requisito Yes/No
1	La Società ha definito una policy privacy e di sicurezza IT compliant alla normativa di settore?	
2	La Società ha nominato un Data Protection Officer (Responsabile della Protezione dei Dati) e ne può indicare i riferimenti?	
3	La Società ha definito una struttura specializzata in ambito privacy, identificando eventuali funzioni preposte per la gestione di eventuali anomalie o violazioni correlate al trattamento dei dati personali?	
4	La Società ha formalizzato un registro dei trattamenti ed è in grado di dimostrarlo?	
5	La Società ha effettuato una valutazione d'impatto (DPIA) al fine di tutelare le libertà e i diritti degli interessati ed è in grado di dimostrarlo?	
6	La Società ha formalizzato una procedura di Incident Management ed è in grado di dimostrarlo?	
7	La Società ha formalizzato una procedura di Data breach ed è in grado di dimostrarlo?	
8	La Società ha definito un Disaster Recovery Plan ed è in grado di dimostrarlo?	
9	La Società ha definito un Business Continuity Plan ed è in grado di dimostrarlo?	
10	La Società ha formalizzato una procedura di Change management ed è in grado di dimostrarlo?	
11	La Società ha messo in atto una procedura per la gestione delle utenze secondo il principio del "need to know" e prevede un sistema di separazione dei compiti e responsabilità in base al servizio richiesto?	
12	La Società ha messo in atto procedure di sicurezza sui dati personali a rischio alto come la cifratura o la pseudonimizzazione?	
13	Se si quali? (indicare nella cella di seguito):	
14	La Società prevede iniziative di formazione e sensibilizzazione nei confronti del personale interno ed esterno (ad esempio consulenti e dipendenti di partner commerciali) circa il corretto utilizzo delle applicazioni e degli strumenti informatici sotto il profilo della privacy/della sicurezza informatica e della riservatezza delle informazioni ed è in grado di documentarlo?	
15	La Società ha censito i propri asset, device mobili aziendali e supporti in ottica privacy? (es. server, pc, tablet, smartphone, chiavette USB).	
	Tali device sono criptati?	
	Se si quali? (indicare nella cella di seguito):	

16	La Società ha messo in atto delle misure per proteggere i locali all'interno dei quali sono contenuti dati personali? (es. sale CED, archivi cartacei,ecc.)	
	Se si quali? (indicare nella cella di seguito):	
17	La Società garantisce gli aggiornamenti di sicurezza dei dispositivi concessi ai propri dipendenti nonché delegati/subfornitori?	
18	La Società dispone di sistemi di difesa perimetrale?	
	Se si quali? (indicare nella cella di seguito):	
19	La Società effettua delle attività di Log Management relativamente alle attività svolte dai propri utenti?	
20	La Società ha adottato dei sistemi di backup che contribuiscono ad innalzare il livello di protezione da perdita di dati personali?	
21	Ne caso in cui il servizio da fornire richiede la connessione per lo scambio di dati personali e critici, la Società dispone di una rete protetta (es. VPN)?	
22	La Società ha provveduto a nominare gli amministratori di sistema in conformità con le disposizioni specifiche in materia adottate dal Garante Privacy italiano?	
23	La Società dispone di un tool di ticketing per la gestione delle abilitazioni, delle change e degli incident a sistema in ottica privacy?	
24	E' possibile produrre una reportistica relativa all'utilizzo di tale tool?	
25	E' prevista una policy di autenticazione e di gestione dell'uso personale delle utenze e password (es. gestione della lunghezza, complessità, durata, conservazione sicura delle password, il censimento delle password tecniche, ecc.) e può provarlo?	
	E' prevista una procedura per la periodica validazione e il censimento delle utenze e delle abilitazioni e può provarlo?	
26	La Società ha nominato dei subfornitori che offrono servizi di supporto in ambito IT e ha previsto delle procedure per la gestione dell'accesso alla rete da parte di questi?	
27	La Società ha effettuato un penetration test negli ultimi 12 mesi?	
28	In caso di fornitura di applicazione e sviluppo delle stesse sono previsti test di sicurezza e può provarlo?	
29	La Società ha subito degli attacchi che hanno comportato la violazione dei dati personali negli ultimi 12 mesi?	
30	La Società effettua periodicamente delle verifiche per valutare la riservatezza, l'integrità, la disponibilità e resilienza dei dati personali?	
31	La Società effettua periodicamente delle verifiche per valutare l'adeguatezza delle misure organizzative e tecniche preposte per la protezione dei dati?	

32	La Società ha ottenuto una delle seguenti certificazioni? - ISAE 3402 (SOC1 e/o SOC2 type 2) - SSA16 (SOC1 e/o SOC2 type 2) - ISO 27001 - ISO 22301	
33	La Società ha ottenuto altre certificazioni in ambito privacy/security? Elencare quali nella cella di seguito:	

Specifica Tecnica 2 - Misure di sicurezza – “ST 2”

L’Appaltatore nominato responsabile esterno al trattamento dei dati assicura di aver adottato le migliori pratiche di settore al fine di garantire un trattamento sicuro dei dati personali e di averle trascritte una propria policy privacy e di sicurezza IT in maniera conforme al Regolamento Europeo n. 679 del 2016, al D. Lgs. 196 del 2003 nonché ai provvedimenti del Garante Privacy emanati, di cui di seguito si delineano aspetti specifici.

1. Disposizioni interne in materia di Privacy

Tra le misure di sicurezza previste in materia di Privacy l’Appaltatore garantisce di:

- aver nominato un Data Protection Officer (Responsabile della Protezione dei Dati) ed aver previsto una struttura specializzata in ambito privacy, identificando eventuali funzioni preposte per la gestione di eventuali anomalie correlate al trattamento dei dati personali. L’Appaltatore garantisce di aver nominato ed investito il personale preposto alla luce delle valutate competenze professionali;

- aver formalizzato un registro dei trattamenti secondo quanto previsto dalla normativa europea in materia di privacy e di aggiornarlo costantemente. L’Appaltatore assicura la corretta tenuta e gestione e permette al Committente di prenderne visione laddove venga richiesto.

- aver effettuato ed effettuare ogni qual volta sia necessario, la valutazione d'impatto (DPIA) al fine di valutare l’esposizione al rischio delle libertà e i diritti degli interessati e di sottoporla alla consultazione del Committente. Inoltre l’Appaltatore garantisce di consultare le Autorità di Controllo qualora gli esiti della valutazione indichino che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio, prima di procedere al trattamento;

- aver definito le misure di sicurezza adeguate ai trattamenti da realizzare, quali ad esempio la pseudonimizzazione e la cifratura dei dati personali, a seguito del censimento dei i propri asset e o device mobili aziendali in ottica privacy (server, pc, tablet, smartphone, chiavette USB). In particolare l’Appaltatore assicura di adottare dei sistemi di backup che contribuiscono ad innalzare il livello di protezione da perdita di dati personali;

- aver formalizzato le seguenti procedure:

- Incident Management;
- Data breach;
- Disaster Recovery Plan;
- Business Continuity Plan;
- Change management;
- Data breach notification.

2. Sicurezza

L’Appaltatore garantisce di proteggere gli accessi ai dati personali, attraverso l’adozione di adeguate misure di sicurezza perimetrale e fisica, nonché la definizione di profili di utenze improntate al principio del "need to know", del minimo privilegio (limitando l’accesso logico a reti, sistemi e data base sulla base delle effettive esigenze operative), della separazione dei compiti.

Inoltre l'Appaltatore garantisce l'utilizzo e la diffusione di policy di autenticazione e di gestione delle password (all'interno delle quali vengano definiti criteri di lunghezza, complessità, durata, conservazione sicura, censimento delle password tecniche, ecc.). La robustezza dei meccanismi di autenticazione e delle password policy deve essere adeguata rispetto al rischio "privacy" identificato dall'Appaltatore nei trattamenti dei dati personali, e quindi, laddove necessario, devono essere più stringenti in termini di sicurezza e controlli rispetto alle disposizioni indicate nell'Allegato B del D. Lgs. 196 del 2003 (Codice Privacy).

L'Appaltatore prevede ed applica procedure per la periodica validazione e il censimento delle utenze e delle abilitazioni.

3. Qualità dei dati e correzione di errori

L'Appaltatore assicura di adottare idonee misure per correggere eventuali errori o inesattezze nei dati personali, nella misura in cui ciò venga richiesto e rientri nell'ambito del Contratto sottoscritto dalle Parti.

4. Formazione e sensibilizzazione del personale preposto

La protezione dei dati aziendali è garantita, oltre che dalle misure tecniche ed organizzative, anche dal corretto comportamento dei soggetti che accedono ai sistemi informatici. Pertanto l'Appaltatore prevede regolarmente e ogni laddove vi sia una modifica normativa, iniziative formative e di sensibilizzazione nei confronti del personale interno ed esterno (ad esempio consulenti e dipendenti di partner commerciali) circa il corretto utilizzo delle applicazioni sotto il profilo della sicurezza informatica.

5. Audit e controlli

L'Appaltatore assicura di condurre periodicamente test autonomi e indipendenti per garantire la conformità alle presenti indicazioni, inclusi gli obblighi di riservatezza, non divulgazione, sicurezza, ripristino in caso di incidente e di porre i risultati alla consultazione del Committente.

3.2 Data Protection Addendum

APPENDIX-COR-ACT-001-I

Notice of appointment of external data processing manager

I. Purpose of this notice

With this notice, Mr. …… in the capacity of. ..... at the Company ..... as Contractor pursuant to contract No. ..... to which this notice is attached, is appointed external data processing manager and as such agrees to perform, in accordance with the instructions of xxxxx, hereinafter the Controller, with registered offices in Via xxxxx, xxx xxxx, xxx - xxxx and on behalf of the latter, the personal data processing operations as defined below.

Mrs. E. Vailati appoints the Company in view of the powers received.

As part of their contractual arrangement, the parties agree to uphold the confidentiality of the data indicated below as well as current regulations applicable to the processing of personal data provided by Legislative Decree No. 196 of 30 June 2003, "Personal Data Protection Code" and by Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016 applicable from 25 May 2018 (hereinafter: GDPR).

II. Description of the processing granted to the Contractor, under art. 28 of the GDPR

The Contractor is authorised to process, in accordance with the instructions of and on behalf of the data Controller, the personal data necessary to provide the services inherent to the contract to which this document is annexed.

In particular, the Contractor will use automated and manual means to process common/anagraphic/legal personal data, as provided by the regulations referred to above, of data subjects such as employees/ex-employees/candidates/suppliers for the purposes provided by the contract and for the duration provided by the contract.

If the Contractor processes data acquired for different purposes, it is considered the autonomous Controller and as such will be liable for any breaches

III. Duration of the contract

Reference shall be made to the contract to which this document is annexed.

IV. Obligations of the Contractor towards the data Controller

In processing the data, the Contractor agrees to comply with the following and with the instructions of the Controller.

If the Contractor considers that an instruction constitutes a breach of the law or of the European regulation on data protection or any other provision of EU law or the legislation of the Member States

relating to data protection, it shall immediately inform the data Controller. Any derogations from the application of technical measures given must be expressly authorised by the Controller.

In addition, if the Contractor is required to transfer data to a third country or to an international organisation governed by EU law or the legislation of the Member State to which it is subject, it is obliged to inform the data Controller before the transfer of the data and indicate which guarantee measures it has adopted from among those provided by GDPR, in particular:

- compliance with the decisions on adequacy, as indicated by art. 45 of the GDPR;
- the adoption of the Standard Contractual Clauses provided for by the European Commission, according to art. 46 of the GDPR.
- the adoption of binding business rules, in accordance with art. 47 of the GDPR.

1. Training of authorised personnel

The Contractor, in accordance with art. 26 of the GDPR, must ensure that the persons authorised to process the personal data provided in the contract:

- agree to abide by the legal obligations of confidentiality;
- have received or receive appropriate training in the field of personal data protection.

2. Documentation that the Contractor makes available to the data Controller

As provided for by art. 28 of the GDPR, the Contractor must provide the data Controller with the necessary documentation to demonstrate compliance with all its obligations and must allow inspections to be carried out by the Controller or by the third party appointed by the latter to perform the audit. The Contractor will be notified of the implementation of the inspections at least 5 working days before the start.

The Contractor must in any case prove that it has adopted the required data protection policy and must conduct standard independent audits in order to ensure compliance with privacy regulatory requirements and with adopted policies. The results of the checks should be made available to the Controller.

The audits must include at least the following areas (a complete list of the control areas required by the data controller is contained in the annex "Technical Specification 1 - List of controls - ST 1".):

- protection of confidentiality, non-disclosure, security;
- privacy risk analysis, as provided by relevant regulations;
- resumption of activities in the event of emergency, as well as business continuity plans and disaster recovery;
- tasks of system administrators, with updated list of appointees including descriptions of their assigned functions.

If the Contractor possesses specific certifications they must make the necessary documentation available to the Controller and ensure their availability for the entire duration of the contract. If by any turn of events the Contractor loses their certification during the execution of the contract, they must promptly notify the Controller and submit a plan that explains the weaknesses that have occurred and the recovery plan envisaged.

The loss of the qualifying requirements may provide cause for termination of the contract.

3. Privacy by design and by default

With regard to tools, products, applications or services, the Contractor must take into consideration the principles of data protection at the design stage as well as during processing (see art. 25 of the GDPR).

4. Appointment of a Subcontractor by the Contractor

Without prejudice to the contractual provisions on the requirement of prior authorisation for subcontracting, the Contractor may ask another party (hereinafter referred to as the "Subcontractor") to carry out a specific data processing task.

In this case, in accordance with art. 28 of GDPR, the Contractor shall inform the Controller that they have appointed in writing the Subcontractor as external data processing manager, providing information that clearly describes the processing tasks assigned to the Subcontractor, the identity and contact information of the Subcontractor and the duration of the contract. The Controller has 15 days from the date of receipt of this information to submit any objections to the information sent by the Contractor regarding the content of the appointment of the Subcontractor as external data processing manager.

The Contractor shall provide the Controller with an updated list of Subcontractors appointed to the processing of the data inherent to the contract to which this notice is annexed.

The Contractor must provide the Subcontractor with the instructions given by the Controller in this notice.The Subcontractor must comply with the obligations under this contract and must process the data in accordance with the instructions given by the Controller to the Contractor.

The Contractor is responsible for ensuring that the Subcontractor has appropriate and sufficient qualifications and capacity to implement the technical and organisational measures in compliance is regulatory requirements. In this regard the Contractor must perform controls on the work of the Subcontractor and ensure the Controller’s access to the documentation produced.

The Contractor shall be fully liable to the Controller if the Subcontractor does not fulfil their obligations to correctly perform the data processing tasks. The Controller reserves the right to carry out audits on the Subcontractor.

5. Obligation of cooperation in relation to the rights of data subjects

The Contractor, in accordance with art. 28 of the GDPR, is obliged to cooperate and support the data Controller as regards mandatory compliance with requests to exercise the rights of the data subject. The Controller is responsible for providing the information required for data protection to persons affected by the data processing at the time of data collection and to make available to the parties concerned an updated list of external managers of the personal data processing.

6. Notification of breaches of personal data

The Contractor, in accordance with the provisions of art. GDPR 33, shall notify the data Controller of every incident and/or breach of personal data without undue delay and within 48 hours of gaining knowledge of the breach, using the following means [indicate address provided for the reception of data breaches].

This notification shall be accompanied by any relevant documentation to ensure that the Controller can, if necessary, inform the competent supervisory authority of the breach.

The documentation must include:

- a description of the nature of the personal data breach including, where possible, the categories and approximate number of the data subjects involved and the categories and approximate number of personal data records affected;
- the name of the person responsible for data protection or another contact who can provide more information;
- a description of the probable consequences of the personal data breach;
- a description of the measures to be adopted to remedy the personal data breach, including, if appropriate, measures to mitigate any negative consequences.

If and to the extent that it is not possible to provide all this information simultaneously, it may be sent at a later time without undue delay.

7. Assistance of the Contractor in fulfilment of obligations of the data Controller

The Contractor shall assist the data Controller in the execution of data protection impact assessments and, if necessary, in the execution of prior consultation with the supervisory authority, in accordance with articles 35 and 36 of the GDPR.

8. Security Measures

The Contractor agrees to implement the security measures identified in the Annex to this notice (See Annex – "Technical Specification 2 - Security Measures – ST 2").

Failure to comply with the measures identified may be cause for termination of the contract.

9. Measures for data processing after the termination of services

As per the instructions and directions stated in art. 28 of the GDPR, the Contractor undertakes to destroy all the personal data processed or transfer it to the Controller, except in the case where the Contractor is obliged to keep the information collected for the protection of legitimate interests (e.g. exercise or defence of a right in court proceedings). In the case of cancellation, the Contractor shall disclose the destruction of all available copies of information systems.If the data is retained, the Contractor shall indicate the reasons and the data retention policy.

10. Keeping a log of processing operations

The Contractor must keep a written log of data processing activities, at least for the processing performed on behalf of the Controller, containing the information requested and indicated by art. 30 of the GDPR. In particular the Contractor is required to retain the following information:

e) the name and contact details of the data processing manager or managers and of each data controller on whose behalf the data processing manager is acting, the representative of the data controller or the data processing manager and, where applicable, of the data protection manager;
f) the categories of processing carried out on behalf of each data controller;
g) where applicable, the transfers of personal data to a third country or an international organisation, including the identification of the third country or international organisation and, in the case of transfers referred to in the second paragraph of Article 49, the documentation of suitable safeguards;
h) where possible, a general description of the technical and organisational security measures referred to in Article 32, paragraph 1.

V. Obligations of the Controller towards the Contractor

The data Controller undertakes to:

4. document in writing all instructions relating to the data processing, to be supplied to the Contractor;
5. ensure, in advance and for the duration of the processing, that other appointed Contractors comply with the obligations pursuant to data protection legislation;
6. supervise the data processing, including the conduct of audits and inspections in respect of the Contractor.

VI. Liability of the Contractor

As provided for by legislation, where the data Controller and the Contractor are involved in the same processing and are considered to be liable for any damage caused to the subjects concerned; each party is jointly and severally liable for the full amount of the damage, in order to guarantee the effective indemnity of the data subject. If the data Controller or the Contractor, as external data processing manager, has paid the full compensation for the damage, that party has the right to claim from the other party involved in the processing the part of the compensation matching their share of the liability for the damage, in accordance with the conditions provided by legislation. For any processing carried out by the Contractor in areas and for purposes other than and not expressly referred to in this notice, it is considered the autonomous Controller and as such is liable for any breaches.

VII. Annexes “Technical Specifications”

- Technical Specification 1 - List of controls - “ST 1”;
- Technical Specification 2 - Security Measures – “ST 2").

Technical Specification 1 - List of controls

ID	Requirements	Requirement met Yes/No
1	Has the Company finalised a privacy and IT security policy pursuant to industry legislation?	
2	Has the Company appointed a Data Protection Officer and can it provide details thereof?	
3	Has the Company defined a specialised structure for the issue of privacy, identifying possible functions for the management of anomalies or breaches in the processing of personal data?	
4	Has the Company formalised a processing log and can it demonstrate it?	
5	Has the Company has made a data processing impact assessment (DPIA) to protect the freedom and the rights of data subjects and can it demonstrate it?	
6	Has the Company formalised an Incident Management procedure and can it demonstrate it?	
7	Has the Company formalised a Data Breach procedure and can it demonstrate it?	
8	Has the Company formalised a Disaster Recovery Plan and can it demonstrate it?	
9	Has the Company formalised a Business Continuity Plan and can it demonstrate it?	
10	Has the Company formalised a Change Management procedure and can it demonstrate it?	
11	Has the Company put in place a user management procedure based on the "need to know" principle and has it arranged a system for the separation of duties and responsibilities on the basis of the service requested?	
12	Has the Company put in place security procedures for high-risk personal data such as encryption or pseudonimization?	
13	If so, which ones? (indicate in the cell below):	
14	Does the Company provide training initiatives and awareness-raising for internal and external staff (e.g. consultants and employees of commercial partners) regarding the correct use of IT applications and tools in the area of privacy/IT security and confidentiality of information and is it capable of documenting it?	
15	Has the Company reviewed its assets, company mobile devices and media in terms of privacy? (e.g. server, pc, tablet, smartphone, USB pendrives).	
	Are these devices encrypted?	
	If so, which ones? (indicate in the cell below):	
16	Has the Company put in place measures to protect the premises containing personal data? (e.g. DCE rooms, paper archives, etc.)	
	If so, which ones? (indicate in the cell below):	

17	Does the Company provide security updates for devices given to their employees and proxies/subcontractors?	
18	Does the Company have perimeter defence systems?	
	If so, which ones? (indicate in the cell below):	
19	Does the Company perform Log Management tasks on the activities of its users?	
20	Has the Company adopted backup systems that help increase protection against loss of personal data?	
21	In cases where the service being provided requires connection for the exchange of personal and critical data, does the Company have a secure network (e.g. VPN)?	
22	Has the Company taken steps to appoint system administrators in accordance with the specific provisions adopted by the Italian Privacy Regulator?	
23	Does the Company have a ticketing tool for the management of system authorisations, changes and incidents from the point of view of privacy?	
24	Is it possible to produce reporting on the use of this tool?	
25	Is there a policy for authentication and management of personal use of userids and passwords (e.g. management of length, complexity, duration, secure storage of passwords, census of technical passwords, etc.) and can you demonstrate it?	
	Is there a procedure for the periodic validation and census of userids and authorisations and can you demonstrate it?	
26	Has the Company appointed sub-suppliers who offer support services in the IT field and has it put in place procedures to manage their access to the network?	
27	Has the Company performed a penetration test in the last 12 months?	
28	In the case of supply of application and development of same, are safety tests in place and can you demonstrate it?	
29	Has the Company suffered attacks that have led to the breach of personal data in the last 12 months?	
30	Does the Company carry out periodic inspections to assess the confidentiality, integrity, availability and resiliency of personal data?	
31	Does the Company carry out periodic inspections to assess the adequacy of the organisational and technical measures for data protection?	
32	Has the Company attained one of the following certifications? - ISAE 3402 (SOC1 and/or SOC2 type 2) - SSA16 (SOC1 and/or SOC2 type 2) - ISO 27001 - ISO 22301	
33	Has the Company attained other privacy/security certifications? List them in the cell below:	

Technical Specification 2 - Security Measures – “ST 2"

The Contractor appointed as external data processing manager declares that it has adopted industry best practices to ensure the secure processing of personal data and that it has incorporated them into an IT privacy and security policy in a manner that complies with European Regulation No. 679 of 2016, Legislative Decree 196 of 2003 and with the measures of the Data Protection Authority, some specific aspects of which are outlined below.

1. Internal provisions for privacy

With regard to privacy security measures, the Contractor declares that:

- it has appointed a Data Protection Officer and has provided for a specialised privacy structure, identifying possible functions for the management of anomalies in the processing of personal data. The Contractor declares that it has appointed and invested the appropriate staff having duly assessed their professional skills;

- has formalised a processing operations log as envisaged by European privacy legislation and undertakes to keep it up to date. The Contractor shall ensure its proper maintenance and management and allows the Client to view it upon request.

- has performed, and performs whenever necessary, an impact assessment (DPIA) to evaluate the risk exposure of the freedom and rights of the data subjects and submits it for review by the Client. In addition, the Contractor undertakes to consult the Supervisory Authority where the assessment outcomes indicate that processing would present a high risk in the absence of measures taken to mitigate the risk, before carrying out the processing;

- has finalised the appropriate processing security measures to be carried out, such as for example the pseudonymization and encryption of personal data, following the survey of the privacy adequacy of its assets and or company mobile devices (servers, PCs, tablets, smartphones, USB pendrives). The Contractor declares that it has adopted backup systems that help increase protection against loss of personal data;

- has formalised the following procedures:

- Incident Management;
- Data breach;
- Disaster recovery plan;
- Business continuity plan;
- Change management;
- Data breach notification.

2. Security

The Contractor declares that it protects access to personal data, through the adoption of: appropriate perimeter and physical security measures; a "need to know” system for the definition of user profiles, the “least privilege” principle (limiting logical access to networks, systems and data bases on the basis of effective operating requirements); and separation of duties.

In addition, the Contractor guarantees the use and dissemination of the policy for authentication and management of passwords (defining the criteria for length, complexity, duration, secure retention, census

of technical passwords, etc.). The robustness of the authentication mechanisms and password policies must be adequate in relation to the privacy risk that the Contractor has identified in the processing of personal data; if necessary, it must be made more stringent in terms of security and controls pursuant to the provisions listed in Annex B of Legislative Decree 196/2003 (Privacy Code).

The Contractor provides for and applies procedures for the periodic validation and review of users and authorisations.

3. Data quality and correction of errors

The Contractor makes sure to adopt appropriate measures to correct any errors or inaccuracies in the personal data, insofar as this is required and is within the scope of the Contract signed by the Parties.

4. Training and awareness-raising of appointed staff

The protection of company data is guaranteed, not only by the technical and organisational measures, but also by the appropriate behaviour of the persons who access the IT systems. Therefore, on a regular basis and whenever regulations change, the Contractor provides training and awareness-raising initiatives for internal and external staff (e.g. consultants and employees of commercial partners) on the correct use of applications for optimised IT security.

5. Audits and controls

The Contractor declares that it conducts regular autonomous and independent tests to ensure compliance with these recommendations, including obligations of confidentiality, non-disclosure, security, recovery in the event of incidents and that it submits the results for review by the Client.

3.3 NUOVA NOMINA/CONTRATTO DEL RESPONSABILE DEL TRATTAMENTO: CONFRONTO TRA DIRETTIVA MADRE E GDPR

Adempimento del Responsabile	Già presente nella Direttiva madre	Introdotto ex novo dal Gdpr
Agisce sulla base di istruzioni **documentate** impartite dal Titolare	x	Nel Gdpr inserito il riferimento al "**documentate**"
Impone obblighi di riservatezza a tutte le persone autorizzate al Trattamento dei Dati personali		x
Adotta misure di sicurezza	x	Concetto di accountability
Rispetta tutte le regole imposte dal Gdpr per nominare dei suoi Responsabili		x
Assiste il Titolare, con misure di sicurezza adeguate, nell'agevolazione dell'esercizio dei diritti e nella soddisfazione delle richieste dell'Interessato		x
Assiste il Titolare nell'ottenimento dell'approvazione delle Anc		x
Cancella o restituisce al Titolare tutti i Dati Personali dopo che è terminata la prestazione dei servizi relativi al Trattamento e cancella le copie esistenti, salvo esista una norma di legge che ne preveda la conservazione		x
Mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Gdpr		x
Consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzati dal Titolare o da un altro soggetto da questi incaricato		x

3.4 Titolare e Responsabile del trattamento a confronto

Cosa prevede la nuova normativa in tema di nomina del Responsabile del trattamento? **Art. 28 GDPR**	La nomina deve avvenire tramite contratto o altro "atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento"
Il contratto tra titolare e responsabile deve prevedere che il Responsabile:	a. tratti i dati personali secondo le **istruzioni** documentate ricevute del titolare del trattamento; b. garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla **riservatezza** o abbiano un adeguato obbligo statutario di riservatezza; c. adotti tutte le **misure (di sicurezza**) richieste ai sensi dell'articolo 32; d. **assista** il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 (misure di sicurezza; notifica di un data breaches; valutazione d'impatto - DPIA; prior-checking), tenendo conto della natura del trattamento e delle informazioni a sua disposizione; e. su indicazione del titolare del trattamento, **cancelli** o gli **restituisca** tutti i dati personali dopo che è terminata la prestazione dei servizi di trattamento di dati e cancelli le copie esistenti; f. metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca agli **audit**, comprese le **ispezioni**, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Titolare del trattamento	Responsabile del Trattamento
Cosa pretendo?	Cosa chiedo/come agisco
Stipulare un contratto con Resp.le	Contratto con indicazione chiara di: 1. durata del trattamento 2. natura e finalità del trattamento 3. tipo di dati personali 4. categorie di interessati 5. obblighi e diritti del responsabile del trattamento
Riservatezza dei dipendenti del Resp.le	Strumento di tutela anche del Resp.le
Conoscere le misure di sicurezza attuate dal Resp.le	Nominare e comunicare Amministratore di Sistema e verifica periodica interna delle sue attività; Indicare contrattualmente le misure esistenti
Supporto dal Resp.le nella compliance al GDPR	Specificare le istruzioni nel contratto
Distruzione/restituzione dati dal Resp.le	Indicazione specifica di cosa vuole il Titolare nel contratto stipulato
Resp.le si sottopone a ispezioni e audit	Specificare che avvengano in ore lavorative e con margine di preavviso
Notifica dal Resp.le di richieste da interessati/Autorità	Informazioni tempestive richiedono un monitoraggio costante: implementare procedure per agire rapidamente
Autorizzazione alla nomina di sub-resp.le/verifica garanzie sufficienti del sub-resp/il Resp.le risponde anche per l'inadempimento del sub-resp.le	Scelta opportuna del sub-resp.le (garanzie sufficienti), con replica nel sub-contratto delle condizioni critiche imposte dal titolare/clausola di manleva da parte del sub-responsabile al Resp.le
Corretta tenuta del Registro dei trattamenti da parte del Resp.le	Corretta tenuta del registro dei trattamenti affinché ci sia corrispondenza esatta con quanto indicato nel contratto
Previsione di una clausola contrattuale in merito al supporto del Resp.le nell'attività di valutazione d'impatto (DPIA) o di preventiva consultazione con l'Autorità Garante (considerando 95)	Indicare nel DPA l'attività di supporto richiesta dal Titolare e gli oneri in capo al Resp.le;
Attività di supporto e collaborazione del Resp.le con il DPO	Indicare nel DPA le figure di riferimento che garantiscano il necessario supporto al DPO incaricato dal Titolare

4. IL TRASFERIMENTO DEI DATI PERSONALI ALL'ESTERO

3.5 NOMINA DEL SUB-RESPONSABILE

Requisiti Regolamentari

- ✓ Preventiva autorizzazione scritta, generica o specifica, da parte del Titolare del Trattamento.
- ✓ Informativa scritta da parte del Responsabile sull'aggiunta di sub-responsabili o modifica degli stessi, nel corso del rapporto.
- ✓ Onere di verifica, a carico del Responsabile e del Titolare, che il sub-responsabile presenti «garanzie sufficienti».
- ✓ Sottoscrizione tra il Responsabile e il sub-responsabile, di un contratto che includa gli stessi obblighi imposti al Responsabile dal Titolare.
- ✓ Di fronte al Titolare, il Responsabile risponde anche degli inadempimenti del sub-responsabile.
- ✓ Sanzione amministrativa pecuniaria, fino al 2% del fatturato mondiale annuo, per le imprese che violano gli obblighi inerenti alla nomina del sub-responsabile.

Approccio

- ✓ Definizione, tra il Titolare e il Responsabile, di un DPA che includa la possibilità per il Responsabile di nominare sub-responsabili. [VEDERE SLIDE SUCCESSIVA PER ESEMPIO DI CLAUSOLA]
- ✓ In caso di autorizzazione generica da parte del Titolare, informativa scritta (PEC) da parte del Responsabile sull'individuazione del sub-responsabile e sull'aggiunta di sub-responsabili o modifica degli stessi, nel corso del rapporto.
- ✓ Eventuale opposizione comunicata per iscritto (PEC) da parte del Titolare alle modifiche o sostituzioni dei sub-responsabili comunicate dal Responsabile.
- ✓ Definizione, tra il Responsabile e il sub-responsabile/sub-responsabili di un DPA, che, con riferimento alla parte di trattamento sub-appaltata al sub-responsabile/sub-responsabili:

a) stabilisca specifici compiti e obblighi a carico del sub-responsabile, gli stessi che gravano sul Responsabile;
b) includa un'ampia manleva da parte del sub-responsabile [VEDERE SLIDE SUCCESSIVA PER ESEMPIO DI MANLEVA]

NOMINA DEL SUB-RESPONSABILE

Esempio di clausola, sulla nomina del sub-responsabile, da inserire nel DPA

[●] [*inserire nome del Responsabile*] si impegna a non nominare un sub-responsabile, in relazione a qualsiasi trattamento, totale o parziale, dei Dati Personali di [●] [*inserire nome del Titolare*], senza previa approvazione scritta di [●] [*inserire nome del Titolare*], nel qual caso [●] [*inserire nome del Responsabile*] e il sub-responsabile/sub-responsabili dovranno sottoscrivere un accordo che includa, a carico del o dei sub-responsabili, gli stessi obblighi in materia di protezione dei dati personali previsti a carico di [●] [*inserire nome del Responsabile*]nel presente DPA. [●] [*inserire nome del Responsabile*] sarà ritenuto pienamente responsabile nei confronti di [●] [*inserire nome del Titolare*] per qualsivoglia atto o omissione del sub-responsabile nell'esecuzione degli obblighi del sub-responsabile in oggetto.

Esempio di clausola di manleva, da parte del su-responsabile al responsabile

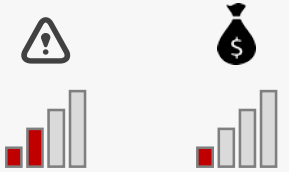
[●] [*inserire nome del sub-responsabile*] manleverà e terrà indenne [●] [*inserire nome del Responsabile*] da qualsivoglia perdita, responsabilità, costi, danni, diretti e indiretti e spese sostenute in relazione a una violazione ad opera del sub-fornitore o dei suoi agenti o sub-fornitori del presente DPA.

3.6 REGISTRO DEI TRATTAMENTI

Legenda: *Copertura rischio (qualitativo)* *Costo di implementazione*

Scenario

Il titolare deve mettere in atto un adeguato approccio di Governance, Risk & Compliance in modo da allineare il contesto aziendale alla nuova normativa.
La finalità principale è la identificazione degli impatti dal punto di vista privacy sul modello di analisi dei rischi e sui controlli interni di compliance, implementando gli strumenti richiesti dalla normativa (Registro trattamenti, Data Protection Impact Assessment)



Medio *Basso*

Obiettivi

- ✓ *Individuazione delle **policy e dei processi** attualmente in essere impattati dalla Normativa per successiva revisione.*
- ✓ ***Classificazione di tutti i rischi identificati** in tema data protection e censimento dei nuovi controlli*
- ✓ *Realizzazione di un **Registro dei Trattamenti** per il titolare e per il Responsabile*
- ✓ *Individuazione di una metodologia di **DPIA** appropriata relativamente all'azienda e al suo mercato*

Approccio

- ✓ *Definizione di un nuovo **framework normativo interno specifico sulla Protezione dei dati** e modifica delle attuali policy impattate*
- ✓ *Aggiornamento del modello di valutazione dei rischi, in modo da includere come fattore critico il Rischio Data Protection*
- ✓ *Creazione e manutenzione di un **Registro dei Trattamenti** (per il Titolre dei dti e per il Responsabile)*
- ✓ *Definizione metodologia e attuazione periodica di un framework di **Data Protection Impact Assesment***
- ✓ *Implementazione di nuovi controlli di compliance normativa in ambito dati personali*
- ✓ *Revisione complessiva dei processi per garantire i nuovi diritti dell'interessato*

REGISTRO DEI TRATTAMENTI (1 DI 2)

SINTESI REQUISITI

Il Regolamento in ambito GDPR prevede la realizzazione del Registro dei Trattamenti, dando indicazioni dei principali requisiti generali con cui costruirlo

Requisiti regolamentari

ESEMPLIFICATIVO

- L'articolo 30 del GDPR si limita ad indicare quali sono gli elementi che il registro deve necessariamente contenere;
- esso, potrebbe comunque essere costituito di più moduli per individuare i trattamenti e gli applicativi/ servizi di riferimento;
- inoltre potrebbe contenere informazioni ulteriori rispetto a quelle obbligatorie sulla base di quanto previsto dal GDPR

Ipotesi di struttura del Registro

- **Processo/macro-attività**
- **Trattamento e finalità del trattamento**
- **Modalità di raccolta del consenso**
- **Categorie di dati trattati e di dati interessati**
- **Termini di conservazione dei dati**
- **Referente interno e categorie di soggetti autorizzati**
- **Responsabili del trattamento (esterni)**
- **Categoria destinatari dei dati**
- **Trasferimento dati personale all'estero**
- **Modalità di trattamento dei dati**
- **Misure di sicurezza tecnico- organizzative**
- **Campi Aggiuntivi**

Il modello è stato disegnato al fine di creare uno strumento che consenta di:

- *garantire la dimostrabilità degli adempimenti normativi*
- *mantenere un collegamento diretto con i principali «oggetti aziendali» (es. mappa dei processi aziendali)*

REGISTRO DEI TRATTAMENTI (2 DI 2)

SINTESI REQUISITI

Il Regolamento in ambito GDPR prevede due tipologie di registro:

Tipologia	Descrizione	Deve contenere
 REGISTRO DEL TITOLARE	Disciplina il registro dei trattamenti del Titolare, stabilendo che **ogni titolare del trattamento** e, ove applicabile, il suo rappresentante, tengono un **registro delle attività di trattamento svolte sotto la propria responsabilità**	• **Il nome e I dati di contatto del Titolare del trattamento** e, ove applicabile, del contitolare del trattamento e del responsabile della protezione dei dati • **L'elenco delle attività di trattamento svolte** sotto la propria responsabilità • **Le finalità del trattamento** • **Una descrizione delle categorie di interessati e delle categorie di dati personali** • Le categorie di destinatari a cui I dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organigrammi internazionali • Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, la documentazione delle garanzie adeguate • Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati • Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative
 REGISTRO DEL RESPONSABILE	Disciplina il registro dei trattamenti del Responsabile, stabilendo che **ogni responsabile del trattamento** e, ove applicabile, il suo rappresentante, tengono un **registro di tutte le categorie di attività relative al trattamento svolto per conto di un Titolare del trattamento**	• **Il nome e I dati di contatto del Responsabile o dei Responsabili del trattamento**, di ogni titolare del trattamento per conto del quale agisce il rappresentante del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e , ove applicabile, del responsabile della protezione dei dati • **Le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento** • Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, la documentazione delle garanzie adeguate • Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative

TITOLARE DEL TRATTAMENTO:

Dati di contatto del titolare:

Rappresentante legale (ove applicabile):

Informazioni obbligatorie richieste dal GDPR – Regolamento Generale sulla Protezione dei Dati

Informazioni aggiuntive non richieste dal GDPR – Regolamento Generale sulla Protezione dei Dati

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

ID	Data Protection Officer* *ove applicabile, i.e. se è stato nominato un DPO	Contitolare/i del trattamento* *ove applicabile, i.e. se è presente uno o più contitolari	Finalità del trattamento	Modalità di raccolta dati	Funzione aziendale	Referente/i intervistato e contatti	Categorie di interessati	Categorie di dati personali	Descrizione dei dati personali	Base Giuridica	Informativa e consenso al trattamento dei dati personali	Data retention period* *ove possibile, i.e. se i dati vengono mantenuti
1												
2												
3												
4												
5												

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Responsabile del Trattamento* *ove applicabile, i.e. dove presente	Categorie di destinatari	Paese in cui risiedono i destinatari	Paese dove risiedono i dati (data centers)/dove i dati sono processati	Condizione per il trasferimento di dati all'interno del paese del Titolare o di un paese dell'UE o di uno stato non UE che assicuri un adeguato livello di protezione* *ove applicabile, i.e. se si sta considerando uno degli scenari suddetti	Condizione per il trasferimento di dati in un paese terzo (non UE) che non assicura un adeguato livello di protezione* *ove applicabile, i.e. se si sta considerando lo scenario indicato	Applicazioni/Sistemi	Referente Applicazione/ Fornitore	Misure di protezione dei dati		
								Descrizione generale delle misure di sicurezza	Descrizione delle misure di sicurezza applicate	Allegati tecnici
						App1				
						App2				
						App1				
						App2				

4. IL TRASFERIMENTO DEI DATI PERSONALI ALL'ESTERO

4.1 Il trasferimento dei dati verso paesi terzi e organizzazioni internazionali: la tutela del dato fuori dai confine UE
4.2 Clausola standard 2010/87 UE per il trasferimento di dati da un Titolare appartenente ad un paese UE a un Responsabile appartenente ad un paese terzo
4.3 Clausola standard 2001/497 UE per il trasferimento di dati da un Titolare appartenente ad un paese UE ad altro Titolare di un paese terzo
4.4 Clausola standard 2001/497 UE per il trasferimento di dati da Responsabile UE a Responsabile extra UE
4.5 Clausola per trasferimento dati extra UE e modello di check list per effettuare la mappatura di eventuali trasferimenti di dati
4.6 Standard Contractual Clauses for the transfer of personal data to processors established in third countries (Commission Decision 2010/87/EU)

4.1 IL TRASFERIMENTO DEI DATI VERSO PAESI TERZI ed ORGANIZZAZIONI INTERNAZIONALI: LA TUTELA DEL DATO FUORI DAI CONFINI U.E.

L'art 3 GDPR traccia l'ambito territoriale di applicazione del Regolamento attraverso l'applicazione congiunta di una serie di criteri che non solo di natura geografica, ma anche logica e di destinazione delle attività.
In particolare l'art. 3 GDPR al paragrafo 1 prevede che il Regolamento si applica nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'UE, indipendentemente dal fatto che tale trattamento sia effettuato o meno nell'UE. Ciò rende necessaria un'attività preliminare volta a definire alcuni fattori, attraverso l'applicazione dei criteri di cui sopra e più precisamente:

- individuare se lo stabilimento è considerato nell'UE, dove per stabilimento si intende non per forza la sede legale, ma una qualsiasi organizzazione stabile, indipendentemente dalla forma giuridica, che svolga un'attività effettiva e reale, anche minima (applicazione del *criterio geografico*);
- stabilire se l'attività si colloca nel contesto delle attività del suddetto stabilimento (applicazione del *criterio di coerenza attività-trattamento*).

Se lo stabilimento che attua il trattamento è collocato nell'UE allora siamo nell'ambito di applicazione del Regolamento, a prescindere dal fatto che il trattamento sia attuato o meno nell'UE

.

L'art 3 GDPR al paragrafo 2 dispone che il Regolamento si applica anche al trattamento dei dati personali di interessati che non si trovano nell'UE quando è effettuato da parte di un titolare del trattamento o responsabile che non è stabilito nell'UE, qualora le attività riguarda l'offerta di beni o prestazione di servizi ai suddetti interessati nell'UE e/o il monitoraggio dei comportamenti degli interessati nella misura vin cui tale comportamento ha luogo all'interno dell'UE

Nell'applicazione di questa seconda disposizione dunque bisognerà valutare se:

- lo stabilimento è in un paese terzo (*criterio geografico*);
- se il trattamento riguarda attività di beni o servizi o attività di monitoraggio di comportamenti nell'Unione (*criterio di coerenza attività-trattamento)*;
- se le attività sono destinate a soggetti che si trovano, anche in via non esclusiva, nell'Unione e l'interessato ne fa parte (*criterio della destinazione a un'utenza geografica*)

Se le risposte saranno affermative, allora saremo anche qui nel campo di applicazione del Regolamento.

Puntualizzata l'area in cui il Regolamento spiega i Suoi effetti, passiamo ora ad esaminare cosa accade quando un titolare/responsabile "trasferisce" i dati verso paesi terzi o organismi internazionali, facendo transitare i dati stessi in area in cui il Regolamento in questione non è più applicabile.

Preliminarmente e tenendo conto che la società è sempre più digitale e interconnessa occorre fare qualche puntualizzazione sul termine "trasferimento", specie con riferimento all'immissione dati in Internet, luogo virtuale e senza confini. A tal proposito vengono d'ausilio le osservazioni della Corte di Giustizia relative al caso Lindqvist la quale è escluso che l'immissione di dati nel web, pur essendo potenzialmente accessibili da soggetti collocati al di fuori dell'UE, non integra un trasferimento di dati verso un paese terzo, sulla scorta del fatto che tali dati "*non sono trasferiti direttamente tra queste due persone, ma attraverso l'infrastruttura informatica del fornitore di servizi di ospitalità presso il quale la pagina è caricata".*

Il trasferimento dei dati personali all'estero è disciplinato dal Titolo V del GDPR ed è volto ad assicurare agli interessati un alto livello di protezione dei propri dati, non inferiore a quello offerto dal diritto dell'U.E. ed evitare, altresì, che il Titolare eluda la regolamentazione europea, trasferendo dati all'estero al mero fine di porre in essere trattamenti non permessi.

L'art. 44 GDPR, infatti, pone il divieto di trasferire dati verso paesi terzi e/o organizzazioni internazionali se non siano rispettate tutte le disposizioni di cui al capo V al fine, appunto, di garantire che il livello di protezione delle persone fisiche

assicurato dal Regolamento non sia pregiudicato e applicando, ad eventuali violazioni, lo stesso rigido sistema sanzionatorio di sui all'art. 83.5 del GDPR (20 000 000 EUR o, per le imprese, fino al 4% del fatturato totale annuo).

A livello operativo, giova qui ricordare che, in ottemperanza del principio di responsabilizzazione, anche i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale devono essere puntualmente identificati ed annotati nel registro dei trattamenti (art. 30.1.e) e 30.2.C)

- Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso senza riserve se la Commissione ha stabilito, mediante una "decisione di adeguatezza", che il paese terzo o l'organizzazione internazionale verso il quale i dati sono diretti garantiscano un livello di protezione adeguato. La decisione può essere revocata, a seguito di riesame periodico ex art. 45.3 GDPR, se il paese terzo o l'organizzazione internazionale non garantiscano più un livello di protezione adeguato secondo i criteri fissati dall'art. 45.2 GDPR.

  Ad oggi i paesi terzi dotati di una "decisione di adeguatezza" sono:

  - Andorra
  - Argentina
  - Australia-PNR
  - Canada
  - Faer Oer
  - Guernsey
  - Isola di Man
  - Israele
  - Jersey
  - Nuova Zelanda
  - Svizzera
  - Uruguay
  - USA-PNR

- La decisione di adeguatezza è però solo uno degli strumenti per poter trasferire i dati all'estero. Infatti, in mancanza delle stesse, il Titolare o il Responsabile che abbia l'esigenza di porre in essere tale trasferimento, può farlo in presenza di "garanzie adeguate" ex art. 46.1.GDPR costituite da:

a) accordi internazionali stipulati tra soggetti pubblici europei e dei paesi terzi. Per essere validi tali accorti non devono porsi in contraddizione con il GDPR, né limitarne la portata, nonché devono essere giuridicamente vincolanti ed avere efficacia esecutiva sia nello Stato terzo sia all'interno dell'UE;

b) utilizzo delle *standard model clause*, adottate dalla Commissione. Esse consistono in testi standard che andranno sottoscritti da ambo le parti e la cui sottoscrizione ritenuta dal legislatore europeo sufficiente per garantire una tutela "sostanzialmente equivalente" a quella che sarebbe garantita ai dati personali nell'Unione, dal punto di vista della protezione e dell'esercizio dei diritti e delle libertà;

c) utilizzo di Clausole tipo di protezione dei dati adottate da un'autorità di controllo (nazionale) e approvate dalla Commissione secondo la medesima procedura d'esame di cui all'art. 93.2 GDPR. Si tratta di una novità introdotta dal GDPR al fine di garantire una omogenea applicazione del GDPR all'interno di ciascuno Stato membro;

d) utilizzo di clausole contrattuali appositamente create dal Titolare o Responsabile del trattamento per il trasferimento dei dati personali nel paese terzo o organizzazione internazionale. Tali contratti, anche se di natura privata, devono essere sottoposti, ai sensi dell'art. 64.4. GDPR, all'autorità di controllo la quale ha il compito di autorizzarne la validità, comunicando altresì la decisione di autorizzazione al comitato per la protezione dei dati affinché possa emettere un parere;

e) utilizzo di disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati. Tali contratti hanno la stessa funzione di quelli previsti tra i privati, con la differenza che, essendo, il campo di applicazione di riferimento i trasferimenti effettuati da autorità o organismi pubblici verso autorità o organismi pubblici di paesi terzi che abbiano analoghi compiti o funzioni, hanno natura di contratto di diritto amministrativo.

4.2 Clausola standard 2010/87 UE per il trasferimento di dati da un Titolare appartenente ad un paese UE a un Responsabile appartenete ad un paese terzo

Ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi che non garantiscono un livello adeguato di protezione dei dati

Nome dell'organizzazione esportatrice: …

Indirizzo: …

Tel. …; Fax …; E-mail: …

Altre informazioni identificative:

…

(«l'esportatore»)

e

Nome dell'organizzazione importatrice: …

Indirizzo: …

Tel. …; Fax …; E-mail: …

Altre informazioni identificative:

…

(«l'importatore»)

denominato ciascuno «parte» e congiuntamente «parti»,

HANNO CONVENUTO le seguenti clausole contrattuali («le clausole») al fine di prestare garanzie sufficienti con riguardo alla tutela della vita privata e dei diritti e delle libertà fondamentali delle persone per il trasferimento dall'esportatore all'importatore dei dati personali indicati nell'appendice 1.

Clausola 1

Definizioni

Ai fini delle presenti clausole:

a) I termini «dati personali», «categorie particolari di dati», «trattamento», «responsabile del trattamento», «incaricato del trattamento», «interessato/persona interessata» e «autorità di controllo» hanno la stessa accezione attribuita nella direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (1);

b) con «esportatore» s'intende il responsabile del trattamento che trasferisce i dati personali;

c) con «importatore» s'intende l'incaricato del trattamento stabilito in un paese terzo che s'impegni a ricevere dall'esportatore dati personali al fine di trattarli per conto e secondo le istruzioni dell'esportatore stesso, nonché a norma delle presenti clausole, e che non sia assoggettato dal paese terzo a un sistema che garantisca una protezione adeguata ai sensi dell'articolo 25, paragrafo 1, della direttiva 95/46/CE;

d) con «subincaricato» s'intende l'incaricato del trattamento designato dall'importatore o da altro suo subincaricato, che s'impegni a ricevere dall'importatore o da altro suo subincaricato dati personali al solo fine di trattarli per conto e secondo le istruzioni dell'esportatore, nonché a norma delle presenti clausole e del subcontratto scritto;

e) con «normativa sulla protezione dei dati» si intende la normativa che protegge i diritti e le libertà fondamentali del singolo, in particolare il diritto al rispetto della vita privata con riguardo al trattamento di dati personali, applicabile ai responsabili del trattamento nello Stato membro in cui è stabilito l'esportatore;

f) con «misure tecniche e organizzative di sicurezza» s'intendono le misure destinate a garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.

Clausola 2

Particolari del trasferimento

I particolari del trasferimento, segnatamente le categorie particolari di dati personali, sono indicati nell'appendice 1 che costituisce parte integrante delle presenti clausole.

Clausola 3

Clausola del terzo beneficiario

1. L'interessato può far valere, nei confronti dell'esportatore, la presente clausola, la clausola 4, lettere da b) a i), la clausola 5, lettere da a) ad e) e da g) a j), la clausola 6, paragrafi 1 e 2, la clausola 7, la clausola 8, paragrafo 2, e le clausole da 9 a 12 in qualità di terzo beneficiario.

2. L'interessato può far valere, nei confronti dell'importatore, la presente clausola, la clausola 5, lettere da a) ad e) e g), la clausola 6, la clausola 7, la clausola 8, paragrafo 2, e le clausole da 9 a 12 qualora l'esportatore sia scomparso di fatto o abbia giuridicamente cessato di esistere, a meno che tutti gli obblighi dell'esportatore siano stati trasferiti, per contratto o per legge, all'eventuale successore che di conseguenza assume i diritti e gli obblighi dell'esportatore, nel qual caso l'interessato può far valere le suddette clausole nei confronti del successore.

3. L'interessato può far valere, nei confronti del subincaricato, la presente clausola, la clausola 5, lettere da a) ad e) e g), la clausola 6, la clausola 7, la clausola 8, paragrafo 2, e le clausole da 9 a 12 qualora sia l'esportatore che l'importatore siano scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi, a meno che tutti gli obblighi dell'esportatore siano stati trasferiti, per contratto o per legge, all'eventuale successore che di conseguenza assume i diritti e gli obblighi dell'esportatore, nel qual caso l'interessato può far valere le suddette clausole nei confronti del successore. La responsabilità civile del subincaricato è limitata ai trattamenti da quello effettuati ai sensi delle presenti clausole.

4. Le parti non si oppongono a che l'interessato sia rappresentato da un'associazione o altra organizzazione, ove siffatta rappresentanza corrisponda alla esplicita volontà dell'interessato e sia ammessa dalla legislazione nazionale.

Clausola 4

Obblighi dell'esportatore

L'esportatore dichiara e garantisce quanto segue:

a) che il trattamento, compreso il trasferimento, dei dati personali, è e continua ad essere effettuato in conformità di tutte le pertinenti disposizioni della normativa sulla protezione dei dati (e viene comunicato, se del caso, alle competenti autorità dello Stato membro in cui è stabilito l'esportatore) nel pieno rispetto delle leggi vigenti in quello Stato;

b) che ha prescritto all'importatore, e continuerà a farlo per tutta la durata delle operazioni di trattamento, di trattare i dati personali trasferiti soltanto per suo conto e conformemente alla normativa sulla protezione dei dati e alle presenti clausole;

c) che l'importatore fornirà sufficienti garanzie per quanto riguarda le misure tecniche e organizzative di sicurezza indicate nell'appendice 2;

d) che, alla luce della normativa sulla protezione dei dati, le misure di sicurezza sono atte a garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali, e che tali misure garantiscono un livello di sicurezza commisurato ai rischi inerenti al trattamento e alla natura dei dati da tutelare, tenuto conto della più recente tecnologia e dei costi di attuazione;

e) che provvederà all'osservanza delle misure di sicurezza;

f) che, qualora il trasferimento riguardi categorie particolari di dati, gli interessati sono stati o saranno informati prima del trasferimento, o immediatamente dopo, che i dati che li riguardano potrebbero essere trasmessi a un paese terzo che non garantisce una protezione adeguata ai sensi della direttiva 95/46/CE;

g) di trasmettere all'autorità di controllo l'eventuale comunicazione presentata dall'importatore o dal subincaricato ai sensi della clausola 5, lettera b), e della clausola 8, paragrafo 3, qualora decida di proseguire il trasferimento o revocare la sospensione;

h) che fornirà, su richiesta degli interessati, copia delle presenti clausole, esclusa l'appendice 2, e una descrizione generale delle misure di sicurezza, nonché copia dei subcontratti aventi ad oggetto il trattamento da effettuarsi in conformità delle presenti clausole, omettendo le

informazioni commerciali eventualmente contenute nelle clausole o nel contratto;

i) che, in caso di subcontratto, il subincaricato svolge l'attività di trattamento in conformità della clausola 11 garantendo un livello di protezione dei dati personali e dei diritti dell'interessato quanto meno uguale a quello cui è tenuto l'importatore ai sensi delle presenti clausole;

j) che provvederà all'osservanza della clausola 4, lettere da a) ad i).

Clausola 5

Obblighi dell'importatore (2)

L'importatore dichiara e garantisce quanto segue:

a) di trattare i dati personali esclusivamente per conto e secondo le istruzioni dell'esportatore, nonché a norma delle presenti clausole, e di impegnarsi a informare prontamente l'esportatore qualora non possa per qualsiasi ragione ottemperare a tale disposizione, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o risolvere il contratto;

b) di non avere motivo di ritenere che la normativa ad esso applicabile impedisca di seguire le istruzioni dell'esportatore o di adempiere agli obblighi contrattuali, e di comunicare all'esportatore, non appena ne abbia conoscenza, qualsiasi modificazione di tale normativa che possa pregiudicare le garanzie e gli obblighi previsti dalle presenti clausole, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o di risolvere il contratto;

c) di aver applicato le misure tecniche e organizzative di sicurezza indicate nell'appendice 2 prima di procedere al trattamento dei dati personali trasferiti;

d) che comunicherà prontamente all'esportatore:

i) qualsiasi richiesta giuridicamente vincolante presentata da autorità giudiziarie o di polizia ai fini della comunicazione di dati personali, salvo che la comunicazione sia vietata da norme specifiche, ad esempio da norme di diritto penale miranti a tutelare il segreto delle indagini;

ii) qualsiasi accesso accidentale o non autorizzato; e

iii) qualsiasi richiesta ricevuta direttamente dagli interessati cui non abbia risposto, salvo che sia stato autorizzato a non rispondere;

e) che risponderà prontamente e adeguatamente a tutte le richieste dell'esportatore relative al trattamento dei dati personali soggetti a trasferimento e che si conformerà al parere dell'autorità di controllo per quanto riguarda il trattamento dei dati trasferiti;

f) che sottoporrà i propri impianti di trattamento, su richiesta dell'esportatore, al controllo dell'esportatore o di un organismo ispettivo composto da soggetti indipendenti, in possesso delle necessarie qualificazioni professionali, vincolati da obbligo di riservatezza e selezionati dall'esportatore, eventualmente di concerto con l'autorità di controllo;

g) che fornirà, su richiesta degli interessati, copia delle presenti, esclusa l'appendice 2, e una descrizione generale delle misure di sicurezza qualora gli interessati non siano in grado di ottenerne copia direttamente dall'esportatore, o copia dei subcontratti del trattamento, omettendo le informazioni commerciali contenute nelle clausole o nel contratto;

h) che, in caso di subcontratto, ha provveduto a informare l'esportatore e ha

da questi ottenuto il consenso scritto;

i) che il subincaricato svolgerà l'attività di trattamento in conformità della clausola 11;

j) che invierà prontamente all'esportatore copia dei subcontratti conclusi ai sensi delle presenti clausole.

Clausola 6

Responsabilità

1. Le parti convengono che l'interessato che abbia subito un pregiudizio per violazione degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera di una parte o del subincaricato ha diritto di ottenere dall'esportatore il risarcimento del danno sofferto.

2. Qualora l'interessato non sia in grado di proporre l'azione di risarcimento di cui al paragrafo 1 nei confronti dell'esportatore per violazione di uno degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera dell'importatore o del subincaricato, in quanto l'esportatore sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, l'importatore riconosce all'interessato stesso il diritto di agire nei suoi confronti così come se egli fosse l'esportatore, a meno che tutti gli obblighi dell'esportatore siano stati trasferiti, per contratto o per legge, all'eventuale successore, nel qual caso l'interessato può far valere i suoi diritti nei confronti del successore.

   L'importatore non può far valere la violazione degli obblighi ad opera del subincaricato al fine di escludere la propria responsabilità.

3. Qualora l'interessato non sia in grado di agire in giudizio, ai fini dei paragrafi 1 e 2, nei confronti dell'esportatore o dell'importatore per violazione di uno degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera del subincaricato, in quanto sia l'esportatore che l'importatore

siano scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi, il subincaricato riconosce all'interessato stesso il diritto di agire nei suoi confronti per quanto riguarda i trattamenti da quello effettuati ai sensi delle presenti clausole così come se egli fosse l'esportatore o l'importatore, a meno che tutti gli obblighi dell'esportatore o dell'importatore siano stati trasferiti, per contratto o per legge, all'eventuale successore, nel qual caso l'interessato può far valere i suoi diritti nei confronti del successore. La responsabilità del subincaricato è limitata ai trattamenti da quello effettuati ai sensi delle presenti clausole.

Clausola 7

Mediazione e giurisdizione

1. L'importatore dichiara che qualora l'interessato faccia valere il diritto del terzo beneficiario e/o chieda il risarcimento dei danni in base alle presenti clausole, egli accetterà la decisione dello stesso interessato:

   a) di sottoporre la controversia alla mediazione di un terzo indipendente o eventualmente dell'autorità di controllo;

   b) di deferire la controversia agli organi giurisdizionali dello Stato membro in cui è stabilito l'esportatore.

2. Le parti dichiarano che la scelta compiuta dall'interessato non pregiudica i diritti sostanziali o procedurali spettanti allo stesso relativamente ai rimedi giuridici previsti dalla normativa nazionale o internazionale.

Clausola 8

Collaborazione con le autorità di controllo

1. L'esportatore si impegna a depositare una copia del presente contratto presso l'autorità di controllo, qualora questa ne faccia richiesta o qualora il deposito sia prescritto dalla normativa sulla protezione dei dati.

2. Le parti dichiarano che l'autorità di controllo ha il diritto di sottoporre a controlli l'importatore e i subincaricati nella stessa misura e secondo le

stesse modalità previste per l'esportatore dalla normativa sulla protezione dei dati.

3. L'importatore informa prontamente l'esportatore dell'esistenza di disposizioni normative applicabili all'importatore o ai subincaricati, che impediscono di sottoporli a controlli ai sensi del paragrafo 2. In tale ipotesi l'esportatore ha facoltà di prendere le misure di cui alla clausola 5, lettera b).

Clausola 9

Legge applicabile

Le presenti clausole sono soggette alla legge dello Stato membro in cui è stabilito l'esportatore, ossia …

Clausola 10

Modifica del contratto

Le parti si impegnano a non alterare o non modificare le presenti clausole. Ciò non osta a che le parti inseriscano altre clausole commerciale ritenute necessarie, purché non siano in contrasto con le clausole.

Clausola 11

Subcontratto

1. L'importatore non può subcontrattare i trattamenti effettuati per conto dell'esportatore ai sensi delle presenti clausole senza il previo consenso scritto dell'esportatore stesso. L'importatore che, con il consenso dell'esportatore, affidi in subcontratto l'esecuzione degli obblighi ai sensi delle presenti clausole stipula, a tal fine, con il subincaricato un accordo scritto che imponga a quest'ultimo gli obblighi cui è egli stesso tenuto in virtù delle clausole (3). L'importatore rimane pienamente responsabile nei confronti dell'esportatore per l'inadempimento, da parte del subincaricato, degli obblighi di protezione dei dati previsti dall'accordo scritto.

2. Nell'accordo scritto tra l'importatore e il subincaricato è inserita la

clausola del terzo beneficiario, di cui alla clausola 3, a favore dell'interessato che non sia in grado di proporre l'azione di risarcimento di cui alla clausola 6, paragrafo 1, nei confronti dell'esportatore o dell'importatore in quanto l'esportatore e l'importatore siano entrambi scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi, e nessun successore abbia assunto, per contratto o per legge, l'insieme dei loro obblighi. La responsabilità civile del subincaricato è limitata ai trattamenti da quello effettuati ai sensi delle presenti clausole.

3. Le disposizioni sulla protezione dei dati ai fini del subcontratto di cui al paragrafo 1 sono soggette alla legge dello Stato membro in cui è stabilito l'esportatore, ossia …

4. L'esportatore tiene un elenco dei subcontratti conclusi ai sensi delle presenti clausole e comunicati dall'importatore a norma della clausola 5, lettera j), e lo aggiorna almeno una volta all'anno. L'elenco sarà tenuto a disposizione dell'autorità di controllo dell'esportatore.

Clausola 12

Obblighi al termine dell'attività di trattamento dei dati personali

1. Le parti convengono che al termine dell'attività di trattamento l'importatore e il subincaricato provvedono, a scelta dell'esportatore, a restituire a quest'ultimo tutti i dati personali trasferiti e le relative copie ovvero a distruggere tali dati, certificando all'esportatore l'avvenuta distruzione, salvo che gli obblighi di legge impediscano di restituire o distruggere in tutto o in parte i dati personali trasferiti. In questo caso, l'importatore si impegna a garantire la riservatezza dei dati personali trasferiti e ad astenersi dal trattare di propria iniziativa tali dati.

2. L'importatore e il subincaricato si impegnano a sottoporre a controllo i propri impianti di trattamento su richiesta dell'esportatore e/o dell'autorità di controllo, ai fini della verifica dell'esecuzione dei

provvedimenti di cui al paragrafo 1.

Per conto dell'esportatore:

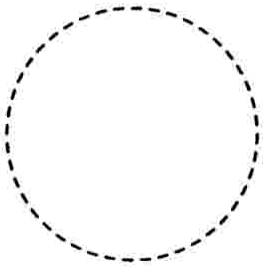
Cognome e nome: …

Qualifica: …

Indirizzo: …

Altre informazioni necessarie per convalidare il contratto:

Firma …



Per conto dell'importatore:

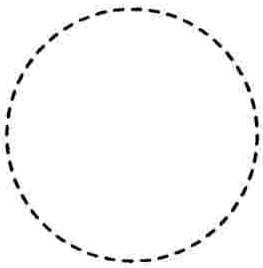
Cognome e nome: …

Qualifica: …

Indirizzo: …

Altre informazioni necessarie per convalidare il contratto:

Firma …



---

(1) Le parti hanno facoltà di avvalersi delle definizioni di cui alla direttiva 95/46/CE nell'ambito della presente clausola se ritenuto preferibile ai fini del contratto.

(2) Disposizioni vincolanti della legislazione nazionale applicabile all'importatore che non vanno oltre quanto è necessario in una società democratica sulla base di uno degli interessi di cui all'articolo 13, paragrafo 1, della direttiva 95/46/CE; in altri termini, le restrizioni necessarie alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate, di un rilevante interesse economico o finanziario dello Stato, della

protezione della persona cui si riferiscono i dati o dei diritti o delle libertà altrui, non sono in contraddizione con le clausole contrattuali tipo. Costituiscono esempi di disposizioni vincolanti che non vanno oltre quanto è necessario in una società democratica le sanzioni internazionalmente riconosciute, gli obblighi di informazione in materia fiscale o contro il riciclaggio di capitali.

(3) Tale prescrizione può considerarsi soddisfatta qualora il subincaricato sottoscriva il contratto concluso tra l'esportatore e l'importatore ai sensi della presente decisione.

Appendice 1

Alle clausole contrattuali tipo

La presente appendice costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti

(Gli Stati membri hanno facoltà di integrare o specificare ulteriormente, conformemente alle rispettive procedure nazionali, qualsiasi altra informazione che debba fare parte della presente appendice)

Esportatore

(specificare brevemente le attività pertinenti al trasferimento):

…

…

…

Importatore

(specificare brevemente le attività pertinenti al trasferimento):

…

…

…

Interessati

I dati personali trasferiti interessano le seguenti categorie di persone (specificare):

…

…

…

Categorie di dati oggetto di trasferimento

I dati trasferiti interessano le seguenti categorie di dati (specificare):

…

…

…

Categorie particolari di dati (se del caso)

Il trasferimento interessa le seguenti categorie particolari di dati (specificare):

…

…

…

Trattamento

I dati personali trasferiti saranno sottoposti alle seguenti attività principali di trattamento (specificare):

…

…

…

L'ESPORTATORE

Nome: …

Firma del rappresentante autorizzato …

L'IMPORTATORE

Nome: …

Firma del rappresentante autorizzato …

Appendice 2

alle clausole contrattuali tipo

La presente appendice costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti

Descrizione delle misure tecniche e organizzative di sicurezza attuate dall'importatore in conformità della clausola 4, lettera d), e della clausola 5, lettera c) (o del documento/atto legislativo allegato):

…

…

…

…

CLAUSOLA ESEMPLIFICATIVA DI INDENNIZZO (FACOLTATIVA)

Responsabilità

Le parti convengono che se una di esse viene riconosciuta responsabile di una violazione delle clausole commessa dall'altra parte, quest'ultima, nei limiti della sua responsabilità, è tenuta a indennizzare la prima per ogni costo, onere, danno, spesa o perdita sostenuti.

Tale indennizzo è subordinato al fatto che:

a) l'esportatore informi prontamente l'importatore in merito alle istanze presentate;

b) l'importatore abbia la possibilità di collaborare con l'esportatore nella difesa e nella risoluzione della controversia

La stessa clausola standard può essere utilizzata quando il Titolare affidi ad un Responsabile, anch'egli stabilito nell'UE, il trattamento dati e quest'ultimo, a sua volta, ricorra ad un fornitore estero per l'esecuzione dei trattamenti demandati.

In quest'ultimo caso, naturalmente, si necessita di alcuni aggiustamenti, primo fra tutti l'inserimento nel contratto tra Titolare e Responsabile di una clausola mandataria, con cui si dà la facoltà al Responsabile di sottoscrivere la *standard clause*, di cui sopra, con il Sub-Responsabile in nome e per conto del Titolare

Tale Clausola potrebbe essere formulata nel seguente modo:

Il Titolare autorizza espressamente il Responsabile, che a ciò si impegna, a stipulare per suo conto con eventuali sub-fornitori, quando stabiliti in un paese al di fuori dell'Unione Europea per il quale la Commissione Europea non abbia emesso un giudizio di adeguatezza del livello di protezione dei dati personali, un accordo per il trasferimento dei dati all'estero contenente le apposite clausole contrattuali (e successive modifiche) adottate dalla stessa Commissione Europea con Decisione 2010/87/EU del 5 febbraio 2010.

4.3 Clausola standard 2001/497 UE per il trasferimento di dati da un Titolare appartenente ad un paese UE ad altro Titolare di un paese terzo

a norma dell'articolo 26, paragrafo 2 della direttiva 95/46/CE per il trasferimento di dati personali a paesi terzi che non garantiscono un livello adeguato di protezione

Nome dell'organizzazione che esporta dati: .....

indirizzo .....

tel.: .....; fax: .....; e-mail: .....

Altre informazioni identificative: .....

("l'esportatore dei dati")

e

Nome dell'organizzazione che importa dati: .....

indirizzo .....

tel.: .....; fax: .....; e-mail: .....

Altre informazioni identificative: .....

("l'importatore dei dati")

HANNO CONVENUTO

le seguenti clausole contrattuali ("le clausole") al fine di addurre salvaguardie adeguate per quanto riguarda la protezione della riservatezza nonché delle libertà e dei diritti fondamentali degli individui per il trasferimento dall'esportatore all'importatore dei dati personali specificati nell'appendice 1.

Clausola 1
Definizioni

Ai fini delle clausole:

(a) "dati personali", "categorie particolari di dati", "trattamento", "responsabile del trattamento", "incaricato del trattamento"," persona interessata" e "autorità di controllo" hanno la stessa accezione di cui alla direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ("la direttiva");

(b) "l'esportatore dei dati" è il responsabile del trattamento che trasferisce i dati personali;

(c) "l'importatore dei dati" è il responsabile del trattamento che accetta di ricevere dati personali dall'esportatore per ulteriore trattamento in conformità alle presenti clausole, e che non è soggetto ad un sistema vigente in un paese terzo per assicurare un'adeguata protezione.

Clausola 2
Particolari del trasferimento

I particolari del trasferimento, e in particolare le categorie di dati personali ed i fini

a cui vengono trasferite, sono specificati nell'appendice 1 che costituisce parte integrante delle presenti clausole.

Clausola 3

Clausola del terzo beneficiario

Le persone interessate dai dati possono chiedere l'esecuzione della presente clausola nonché della clausola 4, lettere b), c) e d), della clausola 5, lettere a), b), c), ed e), della clausola 6, paragrafi 1 e 2, nonché delle clausole 7, 9 e 11 in qualità di terzi beneficiari. Le parti non si oppongono a che le persone interessate dai dati siano rappresentate da un'associazione o da altre organizzazioni se lo desiderano, e se ciò è autorizzato dalla legislazione nazionale.

Clausola 4

Obblighi dell'esportatore dei dati

L'esportatore dei dati s'impegna e garantisce quanto segue:

(a) il trattamento dei dati personali, compreso il loro trasferimento, viene effettuato, e continua ad essere effettuato fino al momento del trasferimento stesso, in conformità a tutte le pertinenti disposizioni (e viene notificato, se del caso, alle autorità competenti) dello Stato membro in cui ha sede l'esportatore, nel pieno rispetto delle leggi vigenti in tale Stato;

(b) qualora il trasferimento riguardi speciali categorie di dati, le persone interessate vengono informate che i dati che li riguardano potrebbero essere trasmessi ad un paese terzo che non fornisce una protezione adeguata, al più tardi all'atto del trasferimento;

(c) mette a disposizione, a richiesta delle persone interessate, copia delle presenti clausole e

(d) risponde entro un termine ragionevole e nella misura del possibile ad eventuali richieste delle autorità di controllo per quanto riguarda il trattamento dei dati personali in questione da parte dell'importatore dei dati, nonché a qualsiasi richiesta delle persone interessate per quanto riguarda il trattamento dei relativi dati da parte dell'importatore degli stessi.

Clausola 5
Obblighi dell'importatore dei dati

L'importatore dei dati s'impegna e garantisce quanto segue:

(a) di non aver ragione di ritenere che la legge applicabile nel suo caso gli impedisca di adempiere agli obblighi di cui al contratto. Qualora la suddetta legge venisse modificata in termini tali da essere probabilmente destinata ad esercitare un sostanziale effetto avverso alle garanzie di cui alle clausole, l'importatore dei dati notifica la variazione all'esportatore dei dati e all'autorità di controllo del paese in cui ha sede l'esportatore. In tal caso l'esportatore dei dati ha diritto di sospendere il trasferimento e/o di rescindere il contratto;

(b) a trattare i dati personali conformemente ai principi obbligatori di tutela dei dati di cui all'appendice 2,

oppure,

su esplicito consenso delle parti espresso barrando le caselle che seguono e fatto salvo il rispetto dei principi obbligatori di protezione dei dati di cui all'appendice 3, a trattare i dati sotto ogni punto di vista rispettando:

- le pertinenti disposizioni di diritto nazionale per la protezione dei diritti e delle libertà fondamentali delle persone fisiche, e in particolare il diritto alla riservatezza

per quanto riguarda il trattamento dei dati personali, applicabili a un responsabile del trattamento nel paese in cui ha sede l'esportatore dei dati,

oppure,

- le pertinenti disposizioni di cui a decisioni della Commissione a norma dell'articolo 25, paragrafo 6 della direttiva 95/46/CE, accertanti che un paese terzo fornisce adeguata protezione soltanto in taluni settori d'attività, purché l'importatore dei dati avente sede in tale paese terzo non sia assoggettabile a dette disposizioni, nella misura in cui le disposizioni stesse siano applicabili nel settore del trasferimento;

(c) a rispondere prontamente e adeguatamente a tutte le ragionevoli richieste dell'esportatore dei dati o delle persone interessate dai dati, per quanto riguarda il trattamento dei dati personali soggetti a trasferimento, a collaborare con la competente autorità di controllo nel corso di tutte le indagini e a rispettare il parere di tale autorità di controllo per quanto riguarda il trattamento dei dati trasferiti;

(d) a sottoporre a controllo, su richiesta dell'esportatore dei dati, i propri servizi di trattamento. Il controllo viene effettuato dall'esportatore dei dati o da un ente ispettivo indipendente e in possesso delle necessarie qualifiche professionali, selezionato dall'esportatore dei dati e, ove necessario, di concerto con le autorità di controllo;

(e) a fornire su richiesta copia delle clausole stipulate alle persone interessate dai dati, e ad indicare la sede competente per eventuali reclami.

Clausola 6
Responsabilità

1. Le parti convengono che le persone interessate dai dati che abbiano subito pregiudizio per qualsiasi violazione delle disposizioni di cui alla clausola 3 hanno

diritto di essere indennizzate dalle parti per il danno sofferto. Le parti convengono che non sussista responsabilità soltanto se dimostrino che nessuna di esse si è resa responsabile di violazioni delle dette disposizioni.

2. L'esportatore e l'importatore dei dati convengono di assumersi separatamente e in solido la responsabilità dei danni causati alle persone interessate dai dati a seguito di violazioni di cui al paragrafo 1. In caso di violazione di dette disposizioni le persone interessate dai dati possono citare in giudizio sia l'esportatore sia l'importatore dei dati, sia entrambi.

3. Le parti concordano che se una di esse viene riconosciuta responsabile di una violazione commessa dall'altra di qualsiasi disposizione di cui al paragrafo 1, la seconda delle parti indennizza la prima per ogni costo, onere, danno, spesa o perdita sostenuta dalla prima, nei limiti che gli sono imputabili.

* (il paragrafo 3 è facoltativo)

Clausola 7
Mediazione e giurisdizione

1. In caso di controversie che non possano essere risolte in via amichevole fra le persone interessate dai dati e una delle parti, e qualora le persone interessate dai dati invochino la disposizione relativa al terzo beneficiario di cui alla clausola 3, le parti convengono di accettare la decisione delle persone interessate dai dati di:

(a) ricorrere alla mediazione ad opera di un terzo indipendente o, se del caso, dell'autorità di controllo;

(b) deferire la controversia ai tribunali dello Stato membro in cui ha sede l'esportatore dei dati.

2. Le parti convengono che, di comune accordo fra le persone interessate dai dati e la relativa controparte, la risoluzione di una specifica controversia possa essere deferita ad un organo arbitrale, purché tale parte abbia sede in un paese che ha ratificato la convenzione di New York sull'applicazione dei lodi arbitrali.

3. Le parti convengono che i paragrafi 1 e 2 si applicano fatti salvi i diritti soggettivi o di azione di cui le persone interessate dai dati possono avvalersi al fine del risarcimento dei danni, in forza di altre disposizioni di diritto nazionale o internazionale.

Clausola 8
Collaborazione con l'autorità di controllo

Le parti convengono di depositare copia del presente contratto presso l'autorità di controllo su richiesta di tale autorità o se tale deposito è previsto dalla legge nazionale.

Clausola 9
Scadenza delle clausole

Le parti convengono che la scadenza delle presenti clausole, in qualsiasi circostanza e per qualsiasi motivo, non esonera le parti stesse dagli obblighi e/o condizioni di cui alle clausole stesse per quanto riguarda il trattamento dei dati trasferiti.

Clausola 10
Legislazione applicabile

Alle presenti clausole si applica la legge dello Stato membro in cui ha sede l'esportatore dei dati.

Clausola 11

Modifica del contratto

Le parti si impegnano a non alterare o modificare i termini qui convenuti delle presenti clausole.

Per conto dell'esportatore dei dati:

Cognome e nome: .....

Qualifica: .....

Indirizzo: .....

Altre eventuali informazioni necessarie per convalidare il contratto: .....

Firma .....

(Sigillo dell'organizzazione)

Per conto dell'importatore dei dati:

Nome (per esteso): .....

Qualifica: .....

Indirizzo: .....

Altre eventuali informazioni necessarie per convalidare il contratto: .....

Firma .....

(Sigillo dell'organizzazione)

4.4 Clausola standard 2001/497 UE per il trasferimento di dati da Responsabile UE a Responsabile extra UE

Accordo di trasferimento di dati

tra

_____

(nome)

_____

(indirizzo e paese di stabilimento)

(d'ora in poi "l'esportatore di dati")

e

_____

(nome)

_____

(indirizzo e paese di stabilimento)

(d'ora in poi "l'importatore di dati"),

ciascuno denominato una "parte", insieme "le parti".

Definizioni

Ai fini delle presenti clausole:

a) "dati personali", "speciali categorie di dati/dati sensibili", "trattamento", "responsabile del trattamento", "incaricato del trattamento", "interessato" e "autorità di controllo/autorità" avranno lo stesso significato indicato nella direttiva 95/46/CE (di conseguenza, si intenderà per "autorità" l'autorità competente in materia di protezione dei dati nel territorio di stabilimento dell'esportatore di dati);

b) per "esportatore di dati" si intende il responsabile del trattamento che

trasferisce i dati personali;

c) per "importatore di dati" si intende il responsabile del trattamento che accetta di ricevere dall'esportatore dati personali per un ulteriore trattamento in conformità con i termini delle presenti clausole e che non è soggetto al sistema di un paese terzo in grado di garantire un'adeguata protezione;

d) per "clausole" si intendono le presenti clausole contrattuali, che costituiscono un documento indipendente che non integra condizioni commerciali stabilite dalle parti in virtù di altri accordi commerciali.

I dettagli del trasferimento (così come i dati personali trasferiti) sono specificati nell'allegato B, che costituisce parte integrante delle presenti clausole.

I. Obblighi dell'esportatore di dati

L'esportatore di dati garantisce e si impegna rispetto a quanto segue:

a) i dati personali sono stati raccolti, trattati e trasferiti in conformità con la legislazione applicabile all'esportatore di dati;

b) l'esportatore ha compiuto ragionevoli sforzi per determinare che l'importatore di dati sia in grado di rispettare gli obblighi giuridici ai quali è tenuto in virtù delle presenti clausole;

c)l'esportatore fornirà all'importatore di dati, se richiesto, copie della legislazione relativa alla protezione di dati del paese in cui è stabilito l'esportatore di dati o i riferimenti a tale legislazione (ove opportuno, ed escludendo la consulenza giuridica);

d)l'esportatore risponderà alle richieste degli interessati e delle autorità relative al trattamento dei dati personali da parte dell'importatore di dati, a meno che le parti non abbiano concordato che sia l'importatore a rispondere a tali richieste. Anche in questo caso, sarà l'esportatore a rispondere, secondo quanto ragionevolmente possibile e a partire dalle informazioni di cui possa ragionevolmente disporre, se l'importatore di dati non è in grado di rispondere o non è disposto a farlo. Le risposte dovranno essere fornite entro un termine ragionevole;

e)l'esportatore metterà a disposizione degli interessati che siano terzi beneficiari ai sensi della clausola III, previa loro richiesta, una copia delle presenti clausole,

a meno che esse contengano informazioni confidenziali, nel qual caso è autorizzato a espungere tali informazioni. Nel caso in cui alcune informazioni siano espunte, l'esportatore di dati informerà per iscritto gli interessati del motivo dell'espunzione e del loro diritto di portare tale espunzione a conoscenza delle autorità. L'esportatore di dati dovrà tuttavia accettare qualunque decisione dell'autorità relativa all'accesso al testo completo delle clausole da parte degli interessati, purché questi ultimi abbiano accettato di rispettare la confidenzialità delle informazioni confidenziali espunte. L'esportatore di dati fornirà all'autorità, previa sua richiesta, una copia delle presenti clausole.

II. Obblighi dell'importatore di dati

L'importatore di dati garantisce e si impegna rispetto a quanto segue:

a) l'importatore attuerà le misure tecniche e organizzative necessarie a proteggere i dati personali contro una distruzione accidentale o illecita o la perdita accidentale, l'alterazione, la divulgazione o l'accesso di soggetti non autorizzati, e a garantire il livello di sicurezza adeguato ai rischi che comportano il trattamento e alla natura dei dati che devono essere protetti;

b) l'importatore avrà messo a punto procedure atte a garantire che qualsiasi terzo cui consenta di accedere ai dati personali, compresi gli incaricati del trattamento, rispetti e mantenga la confidenzialità e la sicurezza dei dati personali. Nessuna persona che operi sotto l'autorità dell'importatore di dati, compresi gli incaricati del trattamento, potrà trattare i dati personali a meno che non abbia ricevuto istruzioni dall'importatore di dati. Questa disposizione non si applica alle persone autorizzate o tenute ad accedere ai dati personali in base alle leggi o ai regolamenti;

c) l'importatore non ha motivo di ritenere, al momento di sottoscrivere le presenti clausole, che esistano atti normativi a carattere locale che possano avere un effetto negativo importante sulle garanzie previste dalle presenti clausole; l'importatore di dati informerà l'esportatore di dati (il quale, quando ne sia richiesto, trasmetterà tale notifica all'autorità) se verrà a conoscenza di un qualunque atto normativo avente tale carattere;

d) l'importatore tratterà i dati personali ai fini descritti nell'allegato B, ed è

giuridicamente abilitato ad offrire le garanzie e a rispettare gli impegni indicati nelle presenti clausole;

e) comunicherà all'esportatore di dati un punto di contatto all'interno della sua organizzazione autorizzato a rispondere alle richieste riguardanti il trattamento dei dati personali e collaborerà in buona fede con l'esportatore di dati, l'interessato e l'autorità nell'ambito di tali inchieste entro un periodo di tempo ragionevole. Nel caso in cui l'esportatore di dati abbia cessato di esistere in diritto, o se così avranno concordato le parti, l'importatore di dati assumerà la responsabilità per quanto riguarda il rispetto delle disposizioni della lettera e) della clausola I;

f) fornirà all'esportatore di dati, su sua richiesta, prove che dimostrino la disponibilità di risorse finanziarie sufficienti a far fronte alle responsabilità cui è tenuto in virtù della clausola III (ad esempio, una copertura assicurativa);

g) metterà a disposizione dietro richiesta ragionevole dell'esportatore di dati, i suoi impianti di trattamento di dati, i suoi archivi e tutta la documentazione necessaria per il trattamento a fini di verifica, audit e/o certificazione.

Queste attività saranno realizzate dall'esportatore di dati (o da un ispettore o revisore imparziale e indipendente designato dall'esportatore di dati e contro il quale non siano state opposte ragionevoli obiezioni dall'importatore di dati) al fine di determinare la conformità con le garanzie previste e gli impegni assunti nelle presenti clausole, con ragionevole preavviso e durante le normali ore lavorative. La richiesta sarà soggetta al consenso o all'approvazione, se necessari, delle autorità di regolamentazione o di vigilanza nel paese dell'importatore. L'importatore farà tutto il possibile per ottenere tale consenso o tale approvazione con tempestività;

h) tratterà i dati personali, a sua discrezione, in conformità con:

i) la legislazione in materia di tutela dei dati del paese nel quale è stabilito l'esportatore di dati;

ii) le disposizioni pertinenti (1) di qualsiasi decisione della Commissione adottata in conformità con il paragrafo 6 dell'articolo 25 della direttiva 95/46/CE, nelle quali si dimostri che l'importatore di dati rispetta le disposizioni pertinenti di tale

autorizzazione o decisione ed è stabilito in un paese nel quale sono applicabili, ma non è coperto dall'autorizzazione o decisione ai fini del trasferimento o dei trasferimenti di dati personali (2); o

iii) i principi relativi al trattamento di dati previsti nell'allegato A.

Opzione scelta dall'importatore di dati:_____

Iniziali dell'importatore di dati: _____;

i) non rivelerà né trasferirà dati personali a terzi responsabili del trattamento stabiliti al di fuori dello Spazio economico europeo (SEE), a meno che notifichi all'esportatore di dati il trasferimento e

i) il terzo responsabile del trattamento sottoponga i dati a trattamento di conformità con una decisione della Commissione nella quale si dichiari che il paese terzo in questione offre la protezione adeguata, o

ii) il terzo responsabile del trattamento sottoscriva queste clausole o qualsiasi altro accordo di trasferimento di dati approvato da un'autorità competente nell'UE, o

iii) gli interessati abbiano avuto la possibilità di opporsi, dopo essere stati informati in merito alle finalità del trasferimento, alle categorie di destinatari e al fatto che i paesi verso i quali i dati vengono esportati potrebbero avere una normativa differente in materia di protezione di dati, o

iv) per quanto riguarda i trasferimenti ulteriori di dati sensibili, gli interessati abbiano dato il loro inequivocabile consenso a tali trasferimenti.

III. Responsabilità e diritti di terzi

a) Ciascuna delle parti sarà responsabile dinnanzi all'altra per i danni provocati dall'inadempimento delle presenti clausole. La responsabilità tra le parti si limiterà al danno realmente sofferto. È specificamente escluso il risarcimento punitivo (vale a dire il risarcimento finalizzato a punire una delle parti per la sua condotta inopportuna o colpevole). Ciascuna delle parti dovrà rispondere dinnanzi agli interessati per i danni provocati da eventuali violazioni dei diritti di terzi nell'ambito delle presenti clausole. Quanto precede fa salva la

responsabilità dell'esportatore in base alla legislazione a lui applicabile in materia di protezione di dati.

b) Le parti concordano che gli interessati, in qualità di terzi beneficiari, potranno invocare di fronte all'importatore o all'esportatore di dati la presente clausola, le lettere b), d) ed e) della clausola I, le lettere a), c), d), e), h) ed i) della clausola II, la lettera a) della clausola III, la clausola V, la lettera d) della clausola VI e la clausola VII per le rispettive violazioni dei loro obblighi contrattuali in rapporto ai loro dati personali; a tal fine, si sottomettono alla giurisdizione del paese di stabilimento dell'esportatore. Nei casi in cui sostenga l'inadempienza da parte dell'importatore di dati, l'interessato dovrà richiedere in primo luogo all'esportatore di avviare azioni adeguate per far valere i suoi diritti nei confronti dell'importatore di dati; se l'esportatore non compie tali azioni entro un termine ragionevole (che nelle normali circostanze sarebbe di un mese), l'interessato potrà far valere i suoi diritti direttamente contro l'importatore di dati. Gli interessati potranno procedere direttamente contro l'esportatore di dati quando questi non abbia compiuto sforzi ragionevoli per determinare se l'importatore di dati sia in grado di rispettare gli obblighi giuridici ai quali è tenuto in virtù delle presenti clausole (ricadrà sull'esportatore di dati l'onere di provare l'effettivo compimento di sforzi ragionevoli).

IV. Legislazione applicabile alle clausole

Le presenti clausole sono soggette alla legislazione del paese nel quale è stabilito l'esportatore di dati, ad eccezione delle disposizioni legali e regolamentari relative al trattamento dei dati personali da parte dell'importatore di dati ai sensi della lettera h) della clausola II, che saranno applicabili solo se l'importatore avrà scelto tale opzione nell'ambito della clausola.

V. Risoluzione di controversie con gli interessati o con l'autorità

a) In caso di controversia o di reclamo presentato contro una o entrambe le parti da un interessato o dall'autorità in merito al trattamento dei dati personali, le parti si informeranno reciprocamente di tali controversie o reclami e collaboreranno al fine di risolverli in modo amichevole quanto prima possibile.

b) Le parti concordano di rispondere a qualsiasi procedura di mediazione non

vincolante e generalmente accessibile che sia stata avviata da un interessato o dall'autorità. Se decidono di partecipare alla procedura, possono farlo a distanza (ad es. per telefono o attraverso altri mezzi elettronici). Le parti concordano inoltre di valutare la possibilità di partecipare a qualsiasi altro procedimento di arbitrato, mediazione o, comunque, di risoluzione delle controversie messo a punto in materia di protezione dei dati.

c) Ciascuna delle parti si impegna ad accettare qualsiasi decisione dei tribunali competenti o dell'autorità del paese di stabilimento dell'esportatore di dati le cui decisioni siano definitive e contro le quali non sia possibile alcun ulteriore appello.

VI. Risoluzione delle clausole

a) Nel caso in cui l'importatore di dati violi gli obblighi ai quali è tenuto in virtù delle presenti clausole, l'esportatore di dati potrà sospendere temporaneamente il trasferimento dei dati personali all'importatore di dati sino a che non venga posto rimedio alla violazione o si concluda il contratto.

b) Nel caso in cui:

i) il trasferimento di dati personali all'importatore di dati sia stato sospeso temporaneamente dall'esportatore di dati per più di un mese in base a quanto previsto dalla lettera a);

ii) il rispetto delle presenti clausole da parte dell'importatore di dati abbia come conseguenza la violazione dei suoi obblighi legali o regolamentari nel paese di importazione;

iii) l'importatore di dati violi in modo sostanziale o persistente una qualche garanzia prevista o un qualche impegno assunto in virtù delle presenti clausole;

iv) una decisione definitiva contro la quale non sia possibile interporre appello dinnanzi a un tribunale competente del paese di stabilimento dell'esportatore di dati o dell'autorità stabilisca che l'importatore o l'esportatore di dati hanno violato le clausole; o

v) sia stata richiesta l'amministrazione giudiziaria o la liquidazione dell'importatore di dati, sia a titolo personale che in qualità di imprenditore, e tale richiesta non sia stata respinta entro il termine previsto dalla legislazione

applicabile; si designi un liquidatore per alcuni dei suoi attivi; si nomini un curatore fallimentare, nel caso in cui l'importatore sia un privato; quest'ultimo abbia richiesto l'avvio di una procedura di concordato; ovvero si trovi in una situazione analoga dinnanzi ad una qualsiasi giurisdizione;

l'esportatore di dati, fatto salvo l'esercizio di qualsiasi altro diritto che possa vantare nei confronti dell'importatore di dati, è autorizzato a risolvere le presenti clausole, nel qual caso informerà l'autorità, se richiesto. Nei casi contemplati ai punti i), ii) o iv), anche l'importatore di dati potrà procedere alla risoluzione.

c) Ciascuna parte può risolvere le presenti clausole se i) la Commissione dichiara che il paese (o parte del suo territorio) verso il quale si trasferiscono i dati e nel quale essi sono trattati dall'importatore di dati garantisce un livello di protezione adeguato in conformità con il paragrafo 6 dell'articolo 25 della direttiva 95/46/CE (o qualsiasi testo che la sostituisca), ovvero ii) la direttiva 95/46/CE (o qualsiasi testo che la sostituisca) divenga direttamente applicabile in tale paese.

d) Le parti concordano che la risoluzione delle presenti clausole in qualsiasi momento, in qualsiasi circostanza e per qualsiasi motivo — ad eccezione della risoluzione in virtù della lettera c) della clausola VI) — non le esime dal rispetto degli obblighi e delle condizioni stabilite nelle presenti clausole per quanto riguarda il trattamento dei dati personali trasferiti.

VII. Modifica delle clausole

Le parti si impegnano a non modificare le presenti clausole se non per aggiornare alcune delle informazioni contenute nell'allegato B, nel qual caso informano l'autorità, dietro sua richiesta. Ciò non impedirà alle parti di aggiungere clausole commerciali aggiuntive ove lo ritengano opportuno.

VIII. Descrizione del trasferimento

I particolari del trasferimento e dei dati personali sono specificati all'allegato B. Le parti concordano che l'allegato B può contenere informazioni commerciali confidenziali che esse non riveleranno a terzi, a meno che non lo esiga la legislazione, ovvero in risposta a un ente regolatore o governativo competente, o quando ciò sia necessario in virtù della lettera e) della clausola I. Le parti potranno introdurre allegati aggiuntivi per regolare trasferimenti aggiuntivi, i

quali saranno presentati all'autorità dietro sua richiesta. Come alternativa, la redazione dell'allegato B potrà essere effettuata in forma tale da coprire trasferimenti multipli.

Data: _____

PER L'IMPORTATORE DI DATI	PER L'ESPORTATORE DI DATI
.....	.....
.....	.....

(1) Per "disposizioni pertinenti" si intendono le disposizioni di un'autorizzazione o decisione che non siano esecutive (le quali sono disciplinate dalle presenti clausole).

(2) Nel caso in cui, tuttavia, si scelga questa opzione, dovranno applicarsi le disposizioni del punto 5 dell'allegato A, relativo ai diritti di accesso, rettifica, cancellazione e obiezione, che prevarranno su qualsiasi disposizione comparabile della decisione della Commissione in questione.

ALLEGATO A

PRINCIPI RELATIVI AL TRATTAMENTO DEI DATI

1. Limitazione dei trasferimenti a una finalità specifica: I dati personali possono essere trattati e successivamente utilizzati o ulteriormente comunicati solo per i fini descritti all'allegato B o autorizzati successivamente dall'interessato.

2. Qualità e proporzionalità dei dati: I dati personali devono essere accurati e, ove necessario, aggiornati. I dati personali devono essere adeguati, pertinenti e non eccedenti in rapporto agli scopi per i quali sono trasferiti e successivamente trattati.

3. Trasparenza: Devono essere fornite agli interessati tutte le informazioni necessarie a garantire il trattamento leale dei dati (così come le informazioni sulla finalità del trattamento e sul possibile trasferimento), a meno che tali informazioni non siano già state fornite dall'esportatore di dati.

4. Sicurezza e confidenzialità: il responsabile del trattamento deve adottare misure tecniche e organizzative volte a garantire il livello di sicurezza adeguato ai rischi che comporta il trattamento dei dati, ad esempio contro la distruzione accidentale o illecita o la perdita accidentale, alterazione, divulgazione o accesso non autorizzati. Le persone che operano sotto l'autorità del responsabile del trattamento, compreso l'incaricato del trattamento, non devono trattare i dati a meno che non ricevano istruzioni del responsabile.

5. Diritti di accesso, rettifica, cancellazione e opposizione: Secondo quanto prevede l'articolo 12 della direttiva 95/46/CE, gli interessati hanno il diritto di conoscere, sia direttamente che attraverso un terzo, i dati personali che su di loro possiede un'organizzazione, ad eccezione delle richieste che configurino chiaramente un abuso di tale diritto, o per il fatto di essere state poste ad intervalli irragionevoli, o a causa del loro numero, o perché hanno natura ripetitiva o sistematica, o ad eccezione dei casi nei quali non è necessario concedere l'accesso all'interessato secondo la legislazione del paese dell'esportatore di dati. A condizione che l'autorità abbia dato la sua previa approvazione, l'accesso può inoltre non essere concesso quando il farlo avrebbe il probabile effetto di danneggiare gravemente gli interessi dell'importatore di dati o di altre organizzazioni che hanno rapporti con l'importatore di dati, e quando tali interessi prevalgono sugli interessi in materia di diritti e di libertà fondamentali dell'interessato. Non sarà necessario determinare l'origine dei dati personali quando ciò non sia possibile mediante sforzi ragionevoli, o se ciò comporterebbe la violazione dei diritti di persone diverse dall'interessato. L'interessato avrà il diritto di far rettificare, modificare o cancellare i dati personali quando essi non siano accurati o il loro trattamento non rispetti i principi stabiliti nel presente allegato. Se vi sono seri motivi di dubitare della legittimità della richiesta, l'organizzazione può richiedere ulteriori giustificazioni prima di procedere alla rettifica, alla modifica o alla cancellazione dei dati. Non sarà necessario notificare la rettifica, la modifica o la cancellazione dei dati ai terzi ai quali essi siano stati rivelati quando ciò richieda uno sforzo sproporzionato. Gli interessati devono inoltre potersi opporre al trattamento dei

dati personali che li riguardano quando esistano motivi seri e legittimi relativi alla loro particolare situazione. L'onere della prova per qualunque rifiuto ricade sull'importatore di dati. L'interessato potrà ricorrere contro un rifiuto dinnanzi all'autorità.

6. Dati sensibili: L'importatore di dati adotta le misure aggiuntive (ad esempio in materia di sicurezza) che risultino necessarie a proteggere i dati sensibili in conformità con gli obblighi ai quali è tenuto in virtù della clausola II.

7. Dati utilizzati a fini di marketing: Quando il trattamento dei dati sia realizzato a fini di marketing diretto, dovranno esistere procedimenti efficaci tali da consentire all'interessato di opporsi in qualsiasi momento a che i suoi dati personali siano utilizzati per gli scopi suddetti.

8. Decisioni automatizzate: Agli effetti del presente allegato, per "decisione automatizzata" si intende una decisione dell'esportatore o dell'importatore di dati che abbia effetti giuridici sull'interessato o che lo interessi in modo significativo e che si basi unicamente su un trattamento automatizzato di dati personali destinato a valutare determinati aspetti della sua personalità, come il suo rendimento lavorativo, la sua solvibilità, l'affidabilità, la condotta, ecc.

L'importatore di dati non adotta nessuna decisione automatizzata relativa agli interessati, eccettuati i casi in cui:

a. i) tali decisioni siano state adottate dall'importatore di dati al momento di stipulare o eseguire un contratto con l'interessato, e

ii) si offra all'interessato l'opportunità di discutere i risultati di una decisione automatizzata che lo riguarda con un rappresentante della parte che abbia adottato la decisione ovvero la possibilità di presentare osservazioni a questa parte;

o

b. la legislazione applicabile all'esportatore di dati stabilisca altrimenti.

ALLEGATO B

DESCRIZIONE DEL TRASFERIMENTO

(Dovrà essere riempito dalle parti)

Interessati

I dati personali trasferiti si riferiscono alle seguenti categorie di interessati:

.....

.....

.....

.....

.....

.....

Finalità del trasferimento o dei trasferimenti

Il trasferimento viene effettuato per le seguenti finalità:

.....

.....

.....

.....

.....

.....

Categorie di dati

I dati personali trasferiti riguardano le seguenti categorie di dati:

.....

.....

.....

.....

.....

.....

Destinatari

I dati personali trasferiti potranno essere forniti unicamente ai seguenti destinatari o categorie di destinatari:

.....

.....

.....

.....

.....

.....

Dati sensibili (se del caso)

I dati personali trasferiti rientrano nelle seguenti categorie di dati sensibili:

.....

.....

.....

.....

.....

.....

Informazioni sulla notificazione presentata dall'esportatore di dati (se applicabile)

.....

.....

.....

Altre inforrnazioni utili (periodo massimo di conservazione e qualsiasi altra informazione pertinente)

.....

.....

.....

Punti di contatto per consultazioni in materia di protezione di dati

Importatore di dati	Esportatore di dati
.....	.....
.....	.....

CLAUSOLE COMMERCIALI ILLUSTRATIVE (OPZIONALI)

Risarcimento tra l'esportatore e l'importatore di dati:

"Ciascuna delle parti risarcisce e manleva l'altra per qualunque costo, onere, danno, spesa o perdita causati all'altra parte in seguito alla violazione di una qualsiasi delle disposizioni delle presenti clausole. L'indennizzo dipenderà dai seguenti elementi: a) la parte o le parti che devono ricevere l'indennizzo (la "parte

indennizzata") notifica immediatamente il reclamo all'altra parte/alle altre parti; b) la parte/le parti che deve/devono provvedere all'indennizzo abbia/abbiano il controllo esclusivo della difesa e della risoluzione di una controversia di questo tipo; e c) la parte indennizzata cooperi ed assista in misura ragionevole la parte indennizzatrice nella difesa del reclamo."

Soluzione delle controversie tra l'esportatore e l'importatore di dati (le parti potranno convenire di sostituire questa clausola con qualsiasi altra clausola di giurisdizione o di soluzione alternativa di conflitti):

"Qualunque controversia tra l'importatore e l'esportatore di dati in rapporto con una supposta violazione di una qualsiasi delle disposizioni delle presenti clausole sarà risolta in via definitiva con riferimento alle norme di arbitrato della Camera di commercio internazionale, da uno o più arbitri designati in conformità con tali norme. La sede dell'arbitrato sarà [ ]. Il numero di arbitri sarà di [ ]."

Attribuzione dei costi:

"Ciascuna parte osserverà gli obblighi ai quali è tenuta in virtù delle presenti clausole a proprie spese."

Clausola aggiuntiva di risoluzione

"In caso di risoluzione delle presenti clausole, l'importatore di dati deve, a discrezione dell'esportatore, restituire immediatamente tutti i dati personali soggetti alle presenti clausole e le copie in suo possesso, ovvero distruggerli completamente e certificare tale circostanza all'esportatore, a meno che la legislazione nazionale o la regolamentazione locale applicabile all'importatore gli impedisca la restituzione o la distruzione totale o parziale di tali dati, nel qual caso l'importatore si impegna a mantenere il segreto sui dati personali e a non sottoporli a ulteriore trattamento per qualsivoglia finalità. L'importatore di dati accetta, su richiesta dell'esportatore di dati, di mettere a disposizione di quest'ultimo o di un ispettore da questi designato e al quale l'importatore di dati non opponga ragionevoli obiezioni, i suoi impianti di trattamento per verificare che ciò sia stato fatto, con ragionevole preavviso e durante l'orario di lavoro."

APPENDICE

alle clausole contrattuali tipo

La presente appendice costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti*.

(*Gli Stati membri hanno facoltà di integrare o specificare ulteriormente, in conformità alle rispettive procedure nazionali, qualsiasi altra informazione che debba fare parte della presente appendice).

Esportatore dei dati

(specificare brevemente le attività pertinenti al trasferimento):

.....

.....

.....

Importatore dei dati

(specificare brevemente le attività pertinenti al trasferimento):

.....

.....

.....

Persone interessate dai dati

I dati personali trasferiti interessano le seguenti categorie di persone (specificare):

.....

.....

.....

Fini del trasferimento

Il trasferimento è necessario ai fini seguenti (specificare):

.....

.....

.....

Categorie di dati oggetto di trasferimento

I dati trasferiti interessano le seguenti categorie di dati (specificare):

.....

.....

.....

Dati delicati (se del caso)

Il trasferimento interessa le seguenti categorie di dati a carattere delicato (specificare):

.....

.....

.....

Destinatari

I dati personali trasferiti possono essere comunicati esclusivamente ai seguenti destinatari o categorie di destinatari (specificare):

.....

.....

.....

Limite di durata

I dati personali trasferiti possono essere conservati soltanto per (specificare): ... (mesi/anni)

L'ESPORTATORE DEI DATI

Nome:..... .....

Firma del rappresentante autorizzato

....

L'IMPORTATORE DEI DATI

Nome:..... .....

Firma del rappresentante autorizzato

....

APPENDICE

alle clausole contrattuali tipo

Principi obbligatori di protezione di cui alla clausola 5, lettera b), primo capoverso

Questi principi di tutela dei dati devono essere letti ed interpretati alla luce delle

disposizioni della direttiva 95/46/CE.

Essi si applicano fatte salve le norme imperative di diritto nazionale, cui sia soggetto l'importatore dei dati, che non eccedano quanto necessario, in una società democratica, per i motivi elencati all'articolo 13, paragrafo 1 della direttiva 95/46/CE, cioè se esse costituiscono misure necessarie alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate, di un rilevante interesse economico o finanziario dello Stato o della protezione della persona interessata o dei diritti e delle libertà altrui.

1) Limitazione del fine - I dati devono essere elaborati e successivamente utilizzati, ovvero ulteriormente comunicati esclusivamente ai fini specificati nell'appendice allegata alle presenti clausole contrattuali tipo. I dati non possono essere detenuti più a lungo di quanto necessario ai fini per cui sono stati trasferiti.

2) Qualità e proporzionalità dei dati - i dati devono essere corretti e, ove necessario, aggiornati. I dati devono essere adeguati, pertinenti e non esuberanti in relazioni ai fini per cui vengono trasferiti e ulteriormente trattati.

3) Trasparenza - gli individui interessati dai dati devono essere informati sui fini del trattamento e sull'identità del responsabile dello stesso nel paese terzo, e su qualsiasi altro aspetto necessario per garantire la correttezza del trattamento, salvo che queste informazioni siano già state fornite dall'esportatore dei dati.

4) Sicurezza e riservatezza - il responsabile del trattamento è tenuto a prendere provvedimenti tecnici ed organizzativi di sicurezza appropriati ai rischi presentati dal trattamento, come accesso non autorizzato. Qualsiasi persona che agisca in virtù dell'autorità del responsabile del trattamento non deve effettuare operazioni di trattamento dei dati se non per disposizione del responsabile del trattamento stesso.

5) Diritti di accesso, rettifica, cancellazione e congelamento dei dati - come previsto dall'articolo 12 della direttiva 95/46/CE, le persone interessate dai dati hanno diritto di accedere a tutti i dati oggetto di trattamento che a loro si riferiscono, nonché il diritto di rettificare, cancellare o bloccare i dati il cui

trattamento non sia conforme ai presenti principi, in particolare per il carattere incompleto o inesatto dei dati stessi.

Le persone interessate dai dati devono inoltre avere la possibilità di opporsi al trattamento dei dati che a loro si riferiscono per validi e legittimi motivi inerenti alla loro situazione particolare.

6) Restrizioni sui trasferimenti successivi - ulteriori trasferimenti di dati personali dall'importatore dei dati ad altri responsabili del trattamento con sede in un paese terzo che non fornisca protezione adeguata o non sia assoggettato a una decisione della Commissione a norma dell'articolo 25, paragrafo 6 della direttiva 96/45/CE (trasferimenti successivi) possono essere effettuati soltanto:

a) se le persone interessate dai dati abbiano dato il loro esplicito consenso al successivo trasferimento in caso si tratti di speciali categorie di dati, o abbiano avuto la possibilità di negare tale consenso negli altri casi.

Le informazioni minime che devono essere fornite alle persone interessate devono comprendere, in una lingua che gli stessi possano capire:

— gli scopi del successivo trasferimento, — l'identità dell'esportatore di dati con sede nella Comunità,

— le categorie degli ulteriori destinatari dei dati con indicazione dei paesi di destinazione, e — l'indicazione che, qualora le persone interessate dai dati approvino il successivo trasferimento, i dati possono essere trattati da un responsabile del trattamento con sede in un paese ove non vi è un livello adeguato di protezione della riservatezza degli individui,

oppure,

b) se l'esportatore e l'importatore dei dati convengano il rispetto delle clausole contrattuali tipo con un altro responsabile del trattamento, che diviene nuova parte contraente delle clausole stesse e assume gli stessi obblighi dell'importatore dei dati.

7) Speciali categorie di dati - nel caso che il trattamento riguardi dati che possano rivelare l'origine razziale o etnica, ovvero le opinioni politiche, le convinzioni religiose o filosofiche, l'adesione a sindacati, dati relativi allo stato di salute o alla vita sessuale, nonché dati relativi a reati, condanne penali o provvedimenti di

sicurezza, devono essere previste ulteriori salvaguardie ai sensi della direttiva 95/46/CE, ed in particolare idonee misure di sicurezza come trasmissione cifrata o registrazione di ogni accesso ai dati.

8) Marketing diretto - quando i dati vengono trattati a fini di marketing diretto, devono essere previste procedure tali da consentire ai soggetti dei dati di negare in qualsiasi momento il proprio consenso all'utilizzazione a tali fini dei dati che li riguardano.

9) Decisioni individuali automatizzate - le persone interessate dai dati hanno il diritto di non essere assoggettati a decisioni basate unicamente sul trattamento automatizzato di dati, a meno che non vengano presi altri provvedimenti per salvaguardare i loro legittimi interessi ai sensi dell'articolo 15 della direttiva 95/46/CE. Qualora l'obiettivo del trasferimento sia una decisione automatizzata ai sensi del citato articolo 15 la persona interessata deve avere il diritto di conoscere le motivazioni su cui si basa detta decisione.

APPENDICE

alle clausole contrattuali tipo

Principi obbligatori di protezione di cui alla clausola 5, lettera b), secondo capoverso

1) Limitazione del fine - I dati devono essere elaborati e successivamente utilizzati, ovvero ulteriormente comunicati esclusivamente ai fini specificati nell'appendice allegata alle presenti clausole contrattuali tipo. I dati non possono essere detenuti più a lungo di quanto necessario ai fini per cui sono stati trasferiti.

2) Diritti di accesso, rettifica, cancellazione e congelamento dei dati - come previsto dall'articolo 12 della direttiva 95/46/CE, le persone interessate dai dati hanno diritto di accedere a tutti i dati oggetto di trattamento che a loro si riferiscono, nonché il diritto di rettificare, cancellare o bloccare i dati il cui trattamento non sia conforme ai presenti principi, in particolare per il carattere incompleto o inesatto dei dati stessi.

Le persone interessate dai dati devono inoltre avere la possibilità di opporsi al trattamento dei dati che a loro si riferiscono per validi e legittimi motivi inerenti

alla loro situazione particolare.

3) Restrizioni sui trasferimenti successivi - ulteriori trasferimenti di dati personali dall'importatore dei dati ad altri responsabili del trattamento con sede in un paese terzo che non fornisca protezione adeguata o non sia assoggettato a una decisione della Commissione a norma dell'articolo 25, paragrafo 6 della direttiva 96/45/CE (trasferimenti successivi) possono essere effettuati soltanto:

a) se le persone interessate dai dati abbiano dato il loro esplicito consenso al successivo trasferimento in caso si tratti di speciali categorie di dati, o abbiano avuto la possibilità di negare tale consenso negli altri casi.

Le informazioni minime che devono essere fornite alle persone interessate devono comprendere, in una lingua che gli stessi possano capire:

— gli scopi del successivo trasferimento, — l'identità dell'esportatore di dati con sede nella Comunità,

— le categorie degli ulteriori destinatari dei dati con indicazione dei paesi di destinazione, e — l'indicazione che, qualora le persone interessate dai dati approvino il successivo trasferimento, i dati possono essere trattati da un responsabile del trattamento con sede in un paese ove non vi è un livello adeguato di protezione della riservatezza degli individui,

ovvero

b) se l'esportatore e l'importatore dei dati convengano il rispetto delle clausole contrattuali tipo con un altro responsabile del trattamento, che diviene nuova parte contraente delle clausole stesse e assume gli stessi obblighi dell'importatore dei dati.

4.5 Clausola di Trasferimento dei dati extra UE

La Società rende noto che il trattamento verso Paesi Terzi avverrà secondo una delle modalità consentite dalla legge vigente, quali ad esempio il consenso dell'interessato, l'adozione di Clausole Standard approvate dalla Commissione Europea, la selezione di soggetti aderenti a programmi internazionali per la libera circolazione dei dati (es. EU-USA Privacy Shield) od operanti in Paesi considerati sicuri dalla Commissione Europea. È possibile avere maggiori informazioni, su richiesta, presso il Titolare o il DPO ai contatti sopraindicati.

Modello di check list per la mappatura dei trasferimenti di dati
Vi è stata adeguata informativa all'interessato in merito al trasferimento dei dati?
Il Paese Terzo è riconosciuto adeguato tramite decisione della Commissione Europea?
Nel caso di assenza di decisione di adeguatezza, il Paese Terzo, per mezzo dei titolari del trattamento, presenta adeguate garanzie di natura contrattuale e pattizia? Gli interessati dispongono di diritti azionabili e mezzi di ricorso effettivi?
Se il Paese Terzo non è ritenuto adeguato rientra il trattamento in uno dei casi di deroga ex art. 49 GDPR?

4.6 Standard Contractual Clauses for the transfer of personal data to processors established in third countries (Commission Decision 2010/87/EU)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.:_____; fax:_____ e-mail:_____

Other information needed to identify the organisation:

……
(the data exporter)

And

Name of the data importing organisation:

Address:

Tel.:_____; fax:_____ e-mail:_____

Other information needed to identify the organisation:

……

(the data importer)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has

factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject

can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is:

……
……..

Data exporter on its own behalf and on behalf of its Affiliates that receive the services referred to in the Data importer

The data importer is:

……
……

Data subjects

The personal data transferred concern the following categories of data subjects:

Unless instructed otherwise by the Data Exporter, data subjects may include Data Exporter and its Affiliates' employees, contractors, business partners, agents, advisor, freelancers, visitors, other individuals, and, to the extent required by law, legal entities whose personal data is processed by Data Importer in its fulfillment of the Agreement.

Categories of data

The personal data transferred concern the following categories of data:

The Data Exporter may submit personal data to the services supplied by the Data Importer, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to the following types of personal data: first and last name; title; position; employer; contact information (company, email, phone, physical business address); ID data; professional life data; personal life data; connection data; localization data; any other data generated by computers system which may identify a data subject; and, in general, any other type of personal data which may be processed from time to time in relation to the services supplied under the Agreement and which shall be specified both in Data Exporter's and in Data Importer's record of processing activities.

Special categories of data

The personal data transferred concern the following special categories of data:

Sensitive data

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Processing necessary to provide the services pursuant with the Agreement

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name:……

Authorised Signature ……

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See regulatory documents related to Privacy and ICT processes

ILLUSTRATIVE INDEMNIFICATION CLAUSE

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.

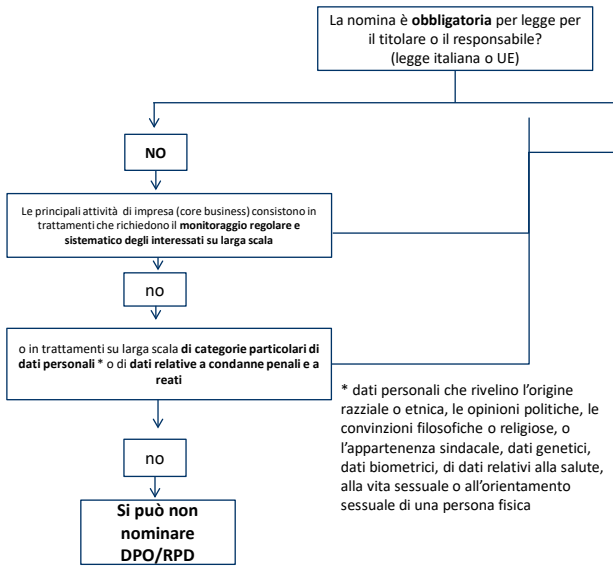
5. DPO - DATA PROTECTION OFFICER

5.1 Il Data Protection Officer

Il Data Protection Officer (DPO), anche detto Responsabile della Protezione dei Dati, è la figura che – per obbligo normativo o per scelta del titolare o del responsabile del trattamento - ha il compito di orchestrare il processo di governance dei trattamenti di dati personali affinché sia conforme alla legge, sovraintendendo alla progettazione, verifica e mantenimento di un sistema organizzato di gestione dei dati, e coadiuvando il titolare/responsabile nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui il titolare/responsabile opera. A tal fine il DPO è chiamato a svolgere un'attività preventiva che include la valutazione d'impatto Privacy delle attività aziendali (c.d. DPIA), il monitoraggio e il tracciamento (registro dei trattamenti), e deve fungere da interlocutore privilegiato all'interno dell'azienda e, all'esterno, con gli interessati e con le istituzioni e l'Autorità Garante.

1. Quando è obbligatorio designare il DPO (in ambito privato)?
    a. Albero decisionale

       Di seguito (e in calce per una migliore lettura) uno schema che illustra i casi in cui è necessario designare un DPO.



Esempi di soggetti tenuti alla nomina secondo il Garante Privacy: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; CAF e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento

2. Designazione del DPO
    a. DPO interno
        i. Nomina del titolare/responsabile – delibera dell'organo esecutivo

           La designazione del DPO esterno può essere preceduta da una nomina da parte del titolare/responsabile (atto unilaterale) e/o da delibera dell'organo esecutivo che, per esempio, a seguito della presentazione del programma di Privacy compliance, dichiara di:

- Di prendere atto che è stato avviato il processo di implementazione e aggiornamento dei documenti richiesti dalla nuova normativa privacy, tra cui l'adozione di procedure/misure organizzative;
- Di approvare il contenuto del Privacy Risk Assessment Report della Società ed in particolare della valutazione del rischio effettuata nonché delle azioni di miglioramento;
- Di approvare il contenuto e l'impostazione degli organigrammi privacy;
- Di procedere alla nomina del DPO, con atto di designazione, avendo individuato in tale soggetto la figura professionale idonea e rispondente ai requisiti dettati dalla normativa vigente;
- (eventuale) di procedere alla nomina del Comitato Privacy (o di altri organi eventualmente previsti).

ii. Atto di designazione

Per la redazione dell'atto di designazione del DPO è utile:

- prendere spunto dalla modello presente sul sito del Garante per la Protezione dei dati personali all'indirizzo: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322273
- consultare le linee guida e le Faq sul Responsabile della Protezione dei Dati in ambito privato o pubblico (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8036793)
- customizzare la nomina sulla base delle esigenze della società, dettagliando i compiti riservati al DPO

In calce, una bozza di atto di designazione con alcuni spunti di integrazione, da modificare in considerazione delle diverse organizzazioni aziendali e da adattare alle singole realtà imprenditoriali e a quanto pattuito con il DPO.

Template atto di designazione DPO.doc

iii. Comunicazione dei dati di contatto del DPO al Garante

La comunicazione prevista dal GDPR (art. 37.7) può essere fatta al Garante solamente online, all'indirizzo https://servizi.gpdp.it/comunicazione-rpd/, e deve essere effettuata dal Legale Rappresentante Titolare/Responsabile del trattamento dei dati, o da un suo delegato con una procedura che prevede l'uso della firma digitale (o firma elettronica qualificata)

b. DPO esterno

i. Nomina del titolare/responsabile – delibera dell'organo esecutivo - contratto

La designazione del DPO esterno può essere preceduta da una nomina da parte del titolare/responsabile (atto unilaterale) e/o da delibera dell'organo

esecutivo e normalmente è preceduta dalla stipula di un contratto con il soggetto esterno a cui è affidato l'incarico di svolgere le attività del DPO.

ii. Contenuto fondamentale del contratto di servizi di DPO:
    - Indicazione del soggetto nominato DPO. Se si tratta di persona giuridica: persone appartenenti al team (tutte godono della tutela riservata al DPO e devono avere le caratteristiche sue proprie), e chiara ripartizione dei compiti all'interno del team DPO
    - Dettagliata descrizione dei compiti affidati al DPO (v. art. 39 GDPR)
    - Tempo dedicato all'attività di DPO
    - Garanzie di autonomia e indipendenza
    - Risorse messe a diposizione del DPO (logistiche, informatiche, economiche)
    - Durata dell'incarico
    - Confidenzialità e riservatezza
    - Manleva

iii. Atto di designazione
    Vedi sopra quanto indicato per il DPO interno , inoltre aver cura di:
    - allineare il contenuto della nomina a quello del contratto stipulato con il DPO

iv. Comunicazione dei dati di contatto del DPO al Garante
    (vedi sopra)

c. Requisiti del DPO

i. Conoscenze (qualifiche professionali) e competenze (capacità di assolvere i compiti)
    Non sono strettamente necessarie specifiche qualifiche o certificazioni per poter svolgere il ruolo di DPO. E' anche possibile che il ruolo del DPO sia svolto da una persona giuridica. Tuttavia, al fine di poter garantire con il grado di professionalità adeguato alla complessità del compito da svolgere, il DPO deve poter dimostrare un adeguato background in termini di:
    - Conoscenza della normativa in materia di protezione dei dati personali (GDPR, linee guida e autorizzazioni Garante Privacy);
    - Conoscenza della normativa specifica del settore di appartenenza dell'impresa (per obbligatorietà trattamenti, data retention ecc.)
    - Conoscenza prassi (provvedimenti e pareri Garante Privacy);
    - Conoscenza aspetti della sicurezza informatica (per verifica dell'adeguatezza delle misure sicurezza)
    - Conoscenza della realtà aziendale, dei processi interni e delle policies dell'azienda, delle politiche e delle prassi di trattamento dei dati personali degli stakeholders dell'impresa (dipendenti, clienti, fornitori, ecc.) e delle relative modalità (es. CRM, profilazione, marketing ecc.)
    - Capacita relazionali, di management, di leadership, di teamwork.

ii. Dotazione delle risorse necessarie da parte del Titolare e del Responsabile del trattamento per assolvere ai propri compiti e per mantenere la propria conoscenza specialistica.
Le indicazioni del WP 29:
- supporto attivo da parte del management;
- tempo sufficiente (se svolge più attività, definire la percentuale di tempo lavorativo per le attività di DPO e il livello di priorità);
- Risorse umane → → da valutare sulla base della struttura aziendale.
Se non è possibile fornire risorse dedicate al DPO, è consigliabile istruire alcune risorse per un supporto (definendo percentuale di tempo lavorativo per l'attività, come per il DPO).
- Risorse finanziarie → non è specificato se al DPO debba essere assegnato un budget di cui poter disporre, ma è consigliabile una previsione in questo senso, anche per provare l'autonomina del DPO.
- Risorse strutturali → deve essere garantito al DPO l'accesso ai servizi della società (HR, IT, legali…)

iii. Collocazione organizzativa
Al fine di poter garantire l'effettività del ruolo e quindi la possibilità di svolgere le funzioni che gli sono demandate dalla legge, al DPO deve essere garantito un adeguato livello di indipendenza e deve riportare o comunque poter aver libero accesso al senior management/vertice aziendale. Il ruolo del DPO è compatibile con altri incarichi, a condizione che non sia in conflitto di interessi. E' quindi preferibile non assegnare il ruolo di DPO a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero con incarichi che implicano il potere di decidere sulle finalità e sulle modalità del trattamento dei dati (es. direzione risorse umane, direzione marketing, direzione finanziaria, responsabile IT ecc.). Da valutare, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (es., il responsabile della funzione legale).

3. DPO di Gruppo
   a. Articolo 37: previsione di un DPO di gruppo a condizione che quest'ultimo sia facilmente raggiungibile da ciascuno stabilimento.
   b. DPO come punto di contatto per gli interessati, l'autorità di controllo, i soggetti interni all'organismo o all'ente.
   c. Compiti del DPO: "informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento".
   d. Rischi:

i. Mancanza di coordinamento in caso di adempimenti che richiedano una reazione rapida a causa della distanza o della comunicazione tra paese e paese.
ii. Difficoltà linguistica di comunicazione con l'Autorità del paese in cui si è verificato un evento di rilevanza Data Protection.
iii. Non perfetta conoscenza della normativa locale di ogni singolo paese.

4. Compiti del DPO
    a. Le attività principali che ricadono sotto il coordinamento del DPO e che, anche in considerazione delle caratteristiche dell'azienda (dimensioni, industry di riferimento, tipo di trattamenti, ecc.) possono richiedere il coinvolgimento di altri ruoli di controllo (per esempio il Compliance Officer, il Risk Manager, l'IT Manager e il responsabile della sicurezza aziendale), sono:
        i. Sorvegliare l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche del titolare/responsabile in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo
        ii. Definire le misure di sicurezza da implementare in relazione ai trattamenti svolti dal titolare/responsabile;
        iii. Formulare gli indirizzi per realizzazione e tenuta del Registro dei trattamenti di cui all'Art. 30 GDPR;
        iv. Fornire indicazioni su eventuali impatti Privacy derivanti da nuove iniziative che si intendono avviare in azienda (con valutazione degli impatti Privacy, c.d. DPIA);
        v. Monitorare il rispetto degli adempimenti Privacy in tutto il ciclo di sviluppo dei sistemi informativi;
        vi. Monitorare l'efficacia delle soluzioni tecniche ed organizzative in uso per la protezione dei dati personali;
        vii. Promuovere la formazione del personale del titolare/responsabile in materia di protezione dei dati personali e sicurezza informatica;
        viii. Coordinare la gestione degli incidenti di sicurezza (c.d. Data Breaches), con le modalità previste da specifica policy del titolare/responsabile;
        ix. Fungere da punto di contatto per il Garante per questioni connesse al trattamento di dati, compresa la consultazione preventiva ove richiesta dalla legge (art. 36 GDPR), e cooperare con il Garante;
        x. Documentare le attività svolte.

5. Gestione rapporti con le autorità (Lead Supervisory Authority)
    a. Lead Supervisory Authority: l´autorità di controllo capofila è l´autorità dello stabilimento principale o unico nell´Ue del Titolare o responsabile del trattamento, alla quale viene trasferita la competenza da tutte le altre autorità di controllo

(definite, in questo caso, "autorità interessate") per quanto riguarda i "trattamenti transfrontalieri" di dati personali svolti da quel titolare o responsabile.

b. Trattamento transfrontaliero di dati personali:
    i. Trattamento dei dati che ha luogo nell'ambito delle attività di stabilimenti in uno o più di uno Stato membro di un Titolare o Responsabile del trattamento dell'Unione ove il Titolare o il Responsabile siano stabiliti in più di uno stato membro, oppure
    ii. Trattamento di dati che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare o responsabile del trattamento nell'unione ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno stato membro
    iii. Le organizzazioni che operano in più di uno stato membro dell'Unione Europea sono chiamate a individuare l'autorità guida ("lead authority") di supervisione alla protezione dei dati.
    iv. L'autorità va ricercata nello stato all'interno della UE in cui risiedono la sede principale e l'amministrazione dell'organizzazione oppure in cui si prendono decisioni in merito ai dati trattati.
        - Diventa così essenziale per il Titolare del trattamento transfrontaliero individuare il luogo dell'amministrazione centrale o dove vengono prese le decisioni relative al trattamento, per poter individuare l'Autorità capofila a cui far riferimento.

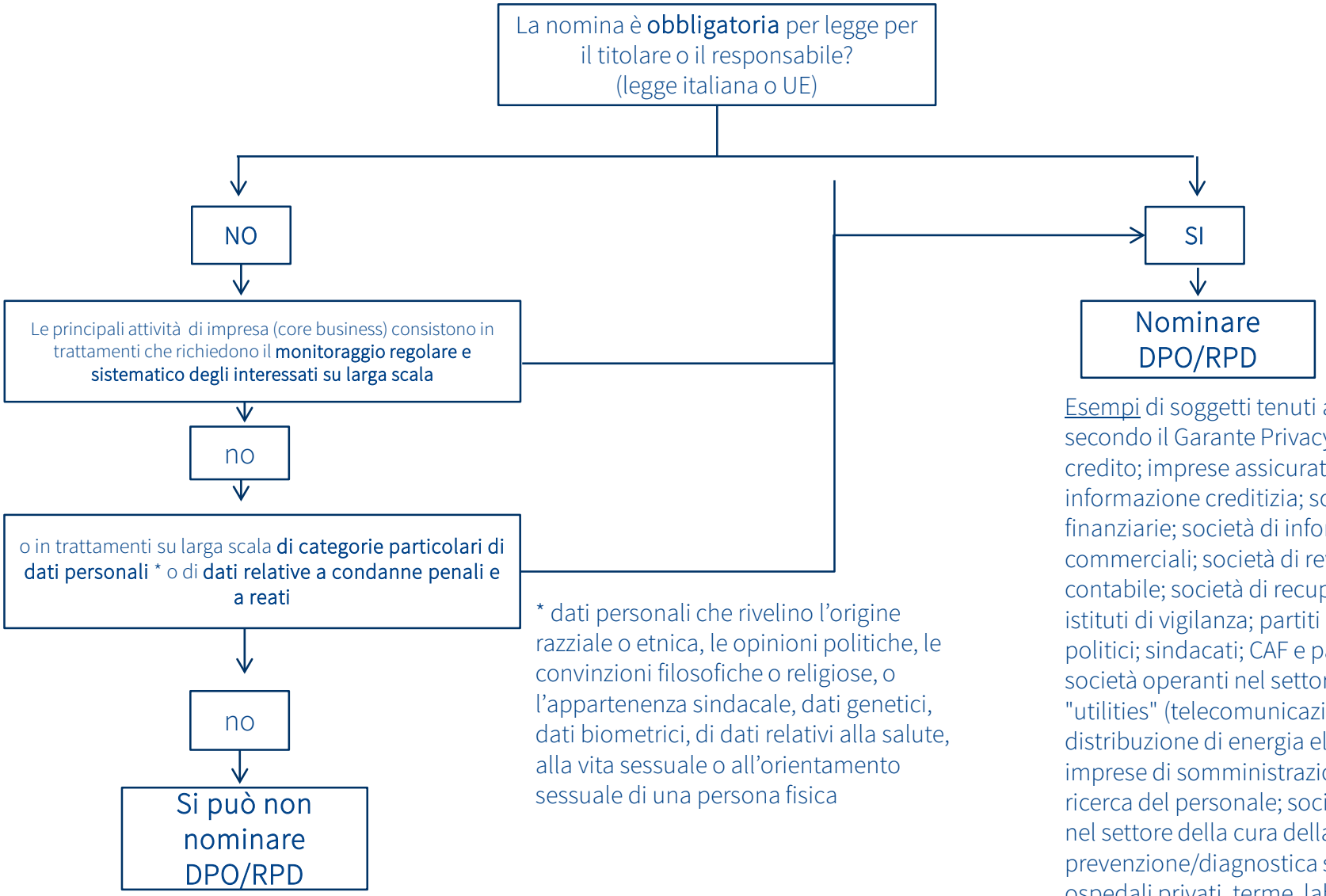
c. Sportello Unico:
    i. L´obiettivo della devoluzione di competenze a favore dell´autorità capofila è garantire l´esistenza di uno "sportello unico" per i trattamenti transfrontalieri di dati personali.
    ii. L' Autorità capofila coopera con le altre autorità interessate, ed avrà la competenza di emettere decisioni vincolanti per le altre autorità. Nel caso in cui il trattamento incida solo su interessi locali, il principio non si applica e la competenza rimane dell'Autorità del paese del trattamento.
    iii. Infine: il WP29 ha preso in esame anche i cosiddetti "borderline cases", cioè le situazioni in cui è estremamente complicato individuare lo stabilimento principale o il luogo in cui le decisioni relative al trattamento vengono prese. In tali casi, la società dovrà designare lo stabilimento che funge da stabilimento principale e, nel caso in cui questo non sia possibile, sarà compito delle Autorità di controllo procedere all'individuazione dello stesso.

6. Gestione pratica delle comunicazioni

   Il DPO è al centro dei flussi comunicativi:

   i. Verso e dall'esterno (Autorità / Interessati al trattamento) → creazione di un canale ad hoc (casella di posta elettronica dedicata, accessibile solo al DPO e a soggetti specifici da lui indicati; recapito postale). Deve essere garantito un monitoraggio giornaliero / a cadenza almeno trisettimanale.

   ii. Verso e nella società / Gruppo –> creazione di un canale interno ad hoc (casella di posta elettronica dedicata / sezione di intranet dedicata; creazione di un repository dove archiviare gli standard privacy della società e documentazione rilevante).



* dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l'appartenenza sindacale, dati genetici, dati biometrici, di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica

Esempi di soggetti tenuti alla nomina secondo il Garante Privacy: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; CAF e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento

Carta intestata della Società

5.2 ATTO DI DESIGNAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (DPO) AI SENSI DELL'ART. 37 DEL REGOLAMENTO UE 2016/679

Premesso che:

- Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*» (di seguito «**GDPR**»), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile dei dati personali (di seguito «**DPO**» o «**RDP**») (artt. 37-39);
- il GDPR prevede l'obbligo per il Titolare o il responsabile del trattamento di designare il DPO quando:

  a) «*il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;*»

  b) «le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;»

  c) «le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.» (art. 37, paragrafo 1);
- le predette disposizioni prevedono che il DPO «*può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi*» (art. 37, paragrafo 6) e deve essere individuato «*in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39*» (art. 37, paragrafo 5) e «*il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento*» (considerando n. 97 del **GDPR**);

Nel caso in cui si opti per la designazione di un DPO condiviso si dovrà aggiungere

- Le disposizioni prevedono inoltre che «*un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione*» (art. 37, paragrafo 3);

- ai sensi dell'art. 4 del GDPR, con il termine «**Titolare del trattamento**» si intende: «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che,*

singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali»;

- la società _____ effettua operazioni di trattamento dei dati personali in qualità di Titolare del trattamento;
- la società _____ ha valutato la necessità di designare il/è tenuto alla designazione obbligatoria del DPO nei termini previsti, rientrando nella fattispecie prevista dall'art. 37, par. 1, lett. a) b) c) del GDPR;

Nel caso in cui si opti per la designazione di un RPD condiviso si dovrà aggiungere

- ha ritenuto di avvalersi della facoltà, prevista dall'art. 37, paragrafo 3, del Regolamento, di procedere alla nomina condivisa di uno stesso RPD con gli *Enti X, Y, Z,* sulla base delle valutazioni condotte di concerto con i predetti Enti in ordine a … (es. dimensioni, affinità tra le relative strutture organizzative, funzioni (attività) e trattamenti di dati personali, razionalizzazione della spesa);

- *l'Ente/la Società* _____all'esito di _____ (*indicare la procedura selettiva interna o esterna, gara, altro*) ha ritenuto che la/il _____, sia in possesso del livello di conoscenza specialistica e delle competenze richieste dall'art. 37, par. 5, del GDPR, per la nomina a DPO, e non si trova in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare;

DESIGNA

(*generalità della persona individuata*) _____, nato a _____, il _____, C.F. _____, con studio/sede in_____, Responsabile della protezione dei dati personali (DPO) per *l'Ente/la Società* _____, con sede in _____, P. IVA _____.

Il predetto _____, in qualità di DPO, nel rispetto di quanto previsto dall'art. 39, par. 1, del GDPR è incaricato di svolgere, in piena autonomia e indipendenza ed in ossequio al segreto professionale e al suo obbligo di riservatezza, i seguenti compiti e funzioni:

a) informare e fornire consulenza al Titolare del trattamento o ai responsabili del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
b) sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o dei responsabili del trattamento in materia di protezione dei dati personali, compresi

Commentato [AV1]: La prima opzione riguarda i casi in cui la società non ricade esattamente nei casi previsti dall'art. 37, ma ha deciso di nominare il DPO su base volontaria. È in ogni caso opportuno che la scelta emerga chiaramente a seguito del privacy assessment e sia debitamente documentata nel relativo materiale (Modello organizzativo, documento di compliance ecc.)

Commentato [AV2]: Scegliere l'opzione di riferimento

Commentato [AV3]: La valutazione dell'adeguatezza delle competenze/conoscenze del DPO deve tenere in considerazione:
- i dati trattati e le esigenze del titolare,
- la frequenza dei trasferimenti al di fuori dell'UE,
- la sua conoscenza del GDPR e delle prassi nazionali ed europee in materia di protezione dati
- la sua conoscenza del settore specifico di attività
- la sua conoscenza della struttura organizzativa
- la sua familiarità con i sistemi informativi
- la sua integrità ed elevati standard deontologici

Commentato [AV4]: È consigliabile esplicitare delle regole interne che garantiscano l'indipendenza del DPO ed evitino i conflitti di interesse.
Il contratto/la nomina del DPO dovrebbe:
- contenere formulazioni specifiche e dettagliate volte a prevenire il conflitto di interessi;
- offrire quante più possibili tutele contro l'ingiusto licenziamento e garantire la stabilità dell'incarico.
In aggiunta, ciascuna organizzazione dovrebbe valutare le qualifiche incompatibili con la nomina a DPO e prevedere un'illustrazione articolata dei casi di conflitti di interessi.

Commentato [AV5]: Può essere nominata DPO anche una persona giuridica, purché ciascun soggetto ad essa appartenente soddisfi tutti i requisiti propri del DPO. È indispensabile indicare chiaramente qual è la ripartizione dei compiti all'interno della struttura.
In ogni caso dovrà essere individuato un unico soggetto, il cui nominativo dovrà essere comunicato al Garante e che fungerà da punto di contatto con l'Autorità.

Commentato [AV6]: È preferibile che il DPO sia localizzato all'interno dell'UE

l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

Tale incarico potrà essere svolto anche attraverso le seguenti attività:

- assistenza nella definizione dei flussi informativi tra il DPO e *l'Ente/la Società* _____;
- assistenza nell'analisi di nuovi progetti e individuazione dei dati trattati, delle problematiche Privacy e delle azioni da porre in essere;
- raccolta di informazioni per individuare i trattamenti svolti;
- analisi e verifica dei trattamenti in termini di loro conformità;
- definizione di un Piano delle Attività;
- predisposizione di una relazione annuale da presentare ai vertici aziendali;
- coordinamento, direzione e partecipazione alle attività e agli incontri del Comitato Privacy e alle riunioni dei Privacy Manager;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR;

d) cooperare con il Garante per la protezione dei dati personali o comunque con l'Autorità di controllo;

e) fungere da punto di contatto con il Garante per la protezione dei dati personali o comunque con l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

(*è possibile inserire di seguito anche ulteriori compiti, purché non incompatibili, quali ad es.:*

a) tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile ed attenendosi alle istruzioni impartite…)

f) adempiere ad ogni ulteriore compito e/o funzione che derivi dalla normativa e dalle procedure aziendali applicabili, tenendo conto anche delle linee guida emanate dalle Autorità in materia di protezione dati personali o da Gruppi di lavoro istituzionali (per es. WP29).

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

La Società _____ si impegna a:

a) mettere a disposizione del RPD le seguenti risorse al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate … (*specificare, ad es. se è stato istituito un apposito Ufficio o gruppo di lavoro, le relative dotazioni logistiche e di risorse umane, nonché i compiti o le responsabilità individuali del personale*);

Commentato [AV7]: Esplicitare quali attività ci si aspetta dal DPO, anche in corrispondenza di come è strutturata l'organizzazione aziendale che si occupa della privacy. Predisporre, se del caso, procedure che indichino quando il DPO deve essere consultato obbligatoriamente.
Si vedano le Linee Guida sui DPO punto 3.1.

Commentato [AV8]: Le linee guida raccomandano di definire chiaramente i compiti del DPO con particolare riguardo alla conduzione della DPIA.
Il titolare del trattamento deve consultarsi con il DPO almeno sulle seguenti tematiche:
- se condurre la DPIA e quale metodo seguire
- se utilizzare risorse interne o esterne
- attenuazione dei rischi per gli interessati
- valutazione dei risultati della DPIA e la loro conformità al GDPR
Il parere del DPO non è vincolante, ma se il titolare se ne discosta deve documentare le ragioni alla base di tale scelta in ossequio al suo obbligo di dimostrare la conformità al regolamento.
v. 4.2 Linee Guida

Commentato [AV9]: Il registro è uno degli strumenti che consentono al DPO di adempiere agli obblighi di sorveglianza, in quanto permette di avere un quadro complessivo dei trattamenti di dati personali svolti. Rimane sempre del titolare la responsabilità della sua tenuta.

Commentato [AV10]: Nella pratica questo si traduce nella stesura di un action plan, buona prassi indicata anche nelle Linee guida sui DPO punti 3.2. e 4.4.

Commentato [AV11]: Il titolare deve coinvolgere il DPO nelle decisioni che impattano sulla protezione dei dati e invitarlo alle riunioni di management.
È inoltre consigliabile individuare il tempo che il DPO dedicherà alla sua attività. Se svolge anche altre funzioni indicare la percentuale del tempo lavorativo che dovrà destinare alla mansione di DPO e definire il livello di priorità delle relative incombenze.
Il titolare deve inoltre garantire al DPO le risorse necessarie (ivi compreso un budget o comunque un potere di spesa da esercitarsi nell'ambito delle procedure aziendali) per assolvere ai suoi compiti, accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Carta intestata della Società

b) non rimuovere o penalizzare il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;
c) garantire che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse;

Commentato [AV12]: Nella pratica ciò significa che non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti e riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

DELIBERA

di designare _____ come Responsabile dei dati personali (DPO) per *l'Ente* _____ .

Il nominativo e i dati di contatto del DPO (recapito postale, telefono, e-mail) saranno resi disponibili nella intranet dell'Ente (url _____, ovvero bacheca) e comunicati al Garante per la protezione dei dati personali. I dati di contatto saranno, altresì, pubblicati sul sito internet istituzionale.

Commentato [AV13]: Indicare tutti i canali messi a disposizione: per es. linea telefonica dedicata.
Favorire la raggiungibilità del DPO da parte di tutte la popolazione aziendale, diffondendo il suo nominativo e i suoi dati di contatto, anche attraverso il suo inserimento negli organigrammi aziendali.

Il DPO rimarrà in carica sino al _____.

Commentato [AV14]: Valutare se inserire questa previsione e determinare la durata della nomina, anche in considerazione delle necessità di stabilità dell'incarico del DPO.

Data …., Luogo ….

Il Titolare del Trattamento

_____

5.3 DPO: struttura e flussi informativi

DPO: STRUTTURA/1

FRAMEWORK NORMATIVO

- GDPR (ART. 38)
- WP29 GUIDELINES ON DPOs, 13 Dec. 2016 (Q&A)

- DPO INTERNO / DPO ESTERNO
- SE INTERNO → EVITARE NOMINE DI SOGGETTI IN «CONFLICTING POSITION»

"Conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues"

- SE ESTERNO → DPO SINGOLO / TEAM DPO + LEAD CONTACT

DPO: STRUTTURA/2

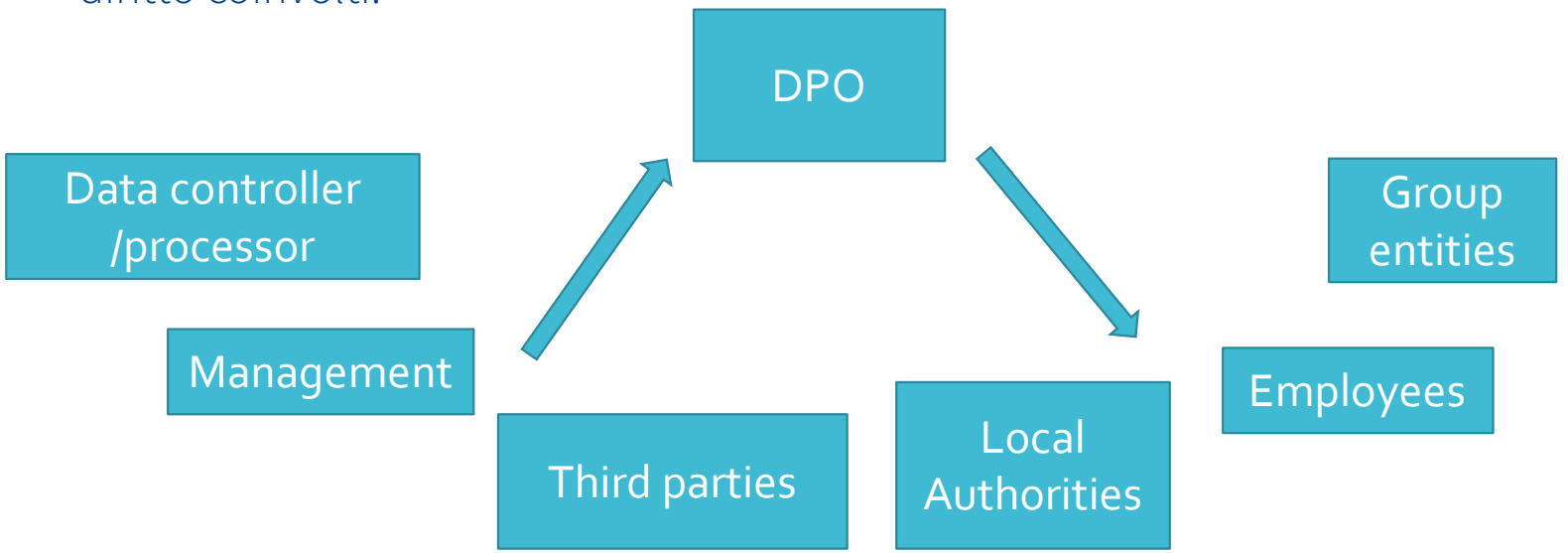
- DPO DI GRUPPO / Più DPO IN UNA LEGAL ENTITY?
- Sì A DPO DI GRUPPO, se effettività
- “If your DPO covers several organisations, they must still be able to perform their tasks effectively, taking into account the structure and size of those organisations. This means you should consider if one DPO can realistically cover a large or complex collection of organisations. You need to ensure they have the necessary resources to carry out their role and be supported with a team, if this is appropriate.”
- “Your DPO must be easily accessible, so their contact details should be readily available to your employees, to the ICO, and people whose personal data you process.” (ICO, DPO Guide to GDPR, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/)

No a “più DPO” ma sì a un “Data protection Specialists’ team”

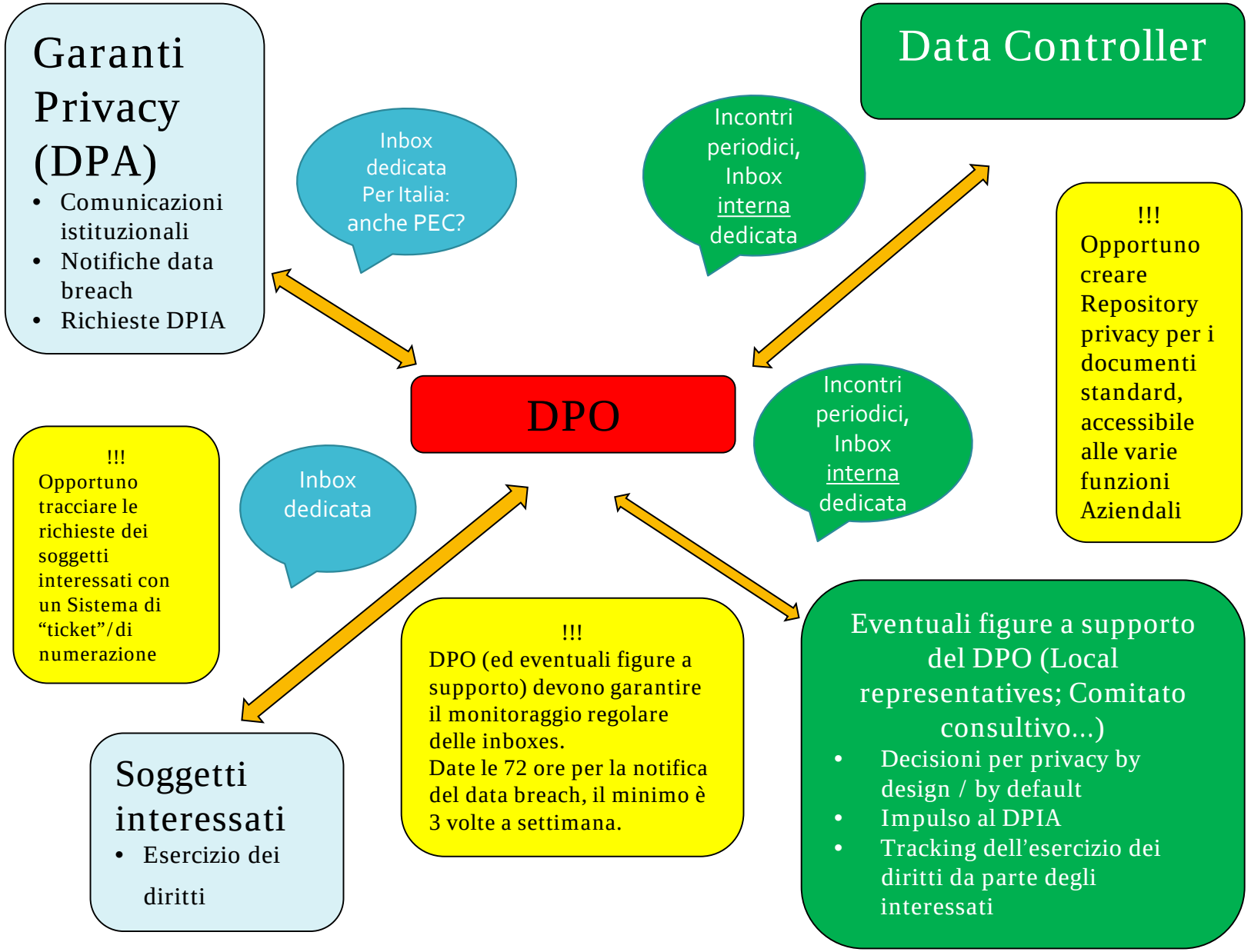
(ICO, DPO Guide to GDPR, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/)

DPO: FLUSSI INFORMATIVI/1

- FRAMEWORK NORMATIVO
- GDPR, artt. 38; 39
- WP ART. 29
- «Easily accessible from each establishment» → canale di contatto disponibile (sia come presenza fisica che attraverso altri mezzi sicuri di comunicazione)
- Lingua: lingua o lingue utilizzate dalle Autorità di vigilanza e dai soggetti di diritto coinvolti.



Comunicazione DA e AL DPO



DPO: struttura e nomina soggetti

- DPO: Designazione tramite delibera CdA
- Comitato: scelto s/base di funzioni maggiormente coinvolte. Figure operative
- + coinvolgimento «a spot» di funzioni investite da specifiche problematiche (es. progettazione «privacy by design»)
- Rappresentanti locali: scelta per cooptazione da top management (necessaria in strutture locali piccole)

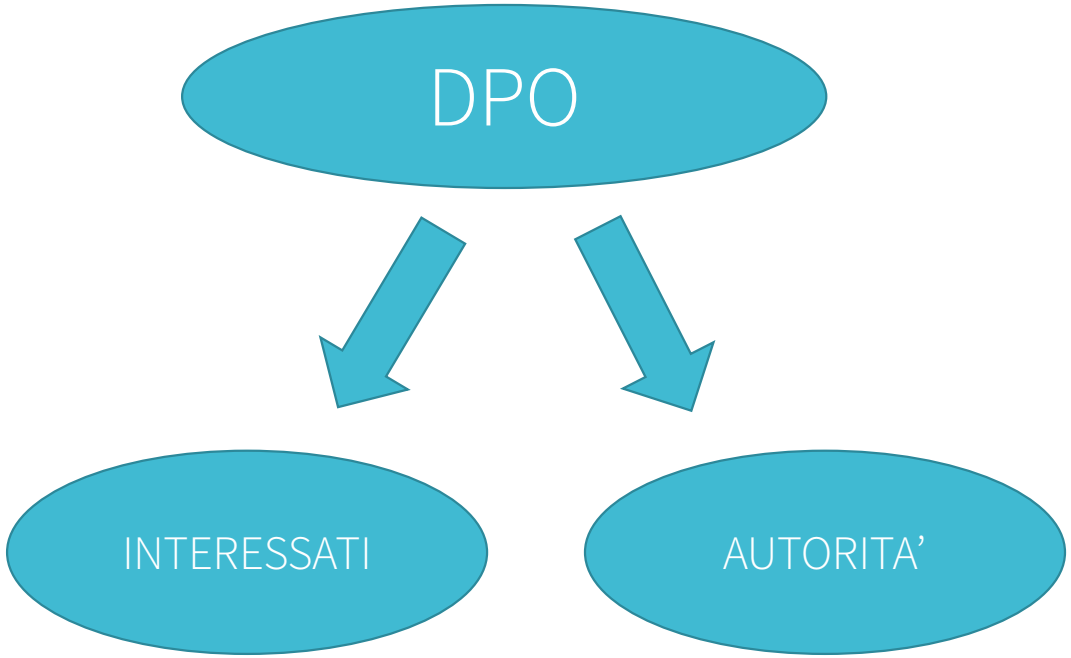
Il DPO nel gruppo di imprese

- L'articolo 37, paragrafo 2, consente a un gruppo imprenditoriale di nominare un unico DPO a condizione che quest'ultimo sia "**facilmente raggiungibile da ciascuno stabilimento**".
- Il concetto di raggiungibilità si riferisce ai compiti del DPO in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente, visto che uno dei compiti del DPO consiste nell' "**informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento**" .

Obblighi del titolare e del responsabile

- L’articolo 38 del GDPR dispone che il titolare e il responsabile del trattamento debbano assicurarsi che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e debbano fornirgli le risorse necessarie per lo svolgimento delle sue funzioni, senza però dargli istruzioni per quanto riguarda l’esecuzione delle stesse.

DPO:



Il DPO deve avere la possibilità di riscontrare tempestivamente questi soggetti

RISCHI:

- Mancanza di coordinamento in caso di adempimenti che richiedano una reazione rapida a causa della distanza o della comunicazione tra paese e paese.
- Difficoltà linguistica di comunicazione con l'Autorità del paese in cui si è verificato un evento di rilevanza Data Protection.
- Non perfetta conoscenza della normativa locale di ogni singolo paese.

LEAD SUPERVISORY AUTHORITY

Trattamento transfrontaliero di dati personali

- Trattamento dei dati che ha luogo nell'ambito delle attività di stabilimenti in uno o più di uno Stato membro di un Titolare o Responsabile del trattamento dell'Unione ove il Titolare o il Responsabile siano stabiliti in più di uno stato membro, oppure
- Trattamento di dati che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare o responsabile del trattamento nell'unione ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno stato membro
- Le organizzazioni che operano in più di uno stato membro dell'Unione Europea sono chiamate a individuare l'**autorità guida** ("**lead authority**") di supervisione alla protezione dei dati.
- L'autorità va ricercata nello stato all'interno della UE in cui risiedono la sede principale e l'amministrazione dell'organizzazione oppure in cui si prendono decisioni in merito ai dati trattati.

definizione

- L´autorità di controllo capofila è l´autorità dello stabilimento principale o unico nell´Ue del Titolare o responsabile del trattamento, alla quale viene trasferita la competenza da tutte le altre autorità di controllo (definite, in questo caso, "autorità interessate") per quanto riguarda i "trattamenti transfrontalieri" di dati personali svolti da quel titolare o responsabile.

Trattamento transfrontaliero di dati personali

- Diventa così essenziale per il Titolare del trattamento transfrontaliero individuare il luogo dell'amministrazione centrale o dove vengono prese le decisioni relative al trattamento, per poter individuare l'Autorità capofila a cui far riferimento.

Sportello Unico

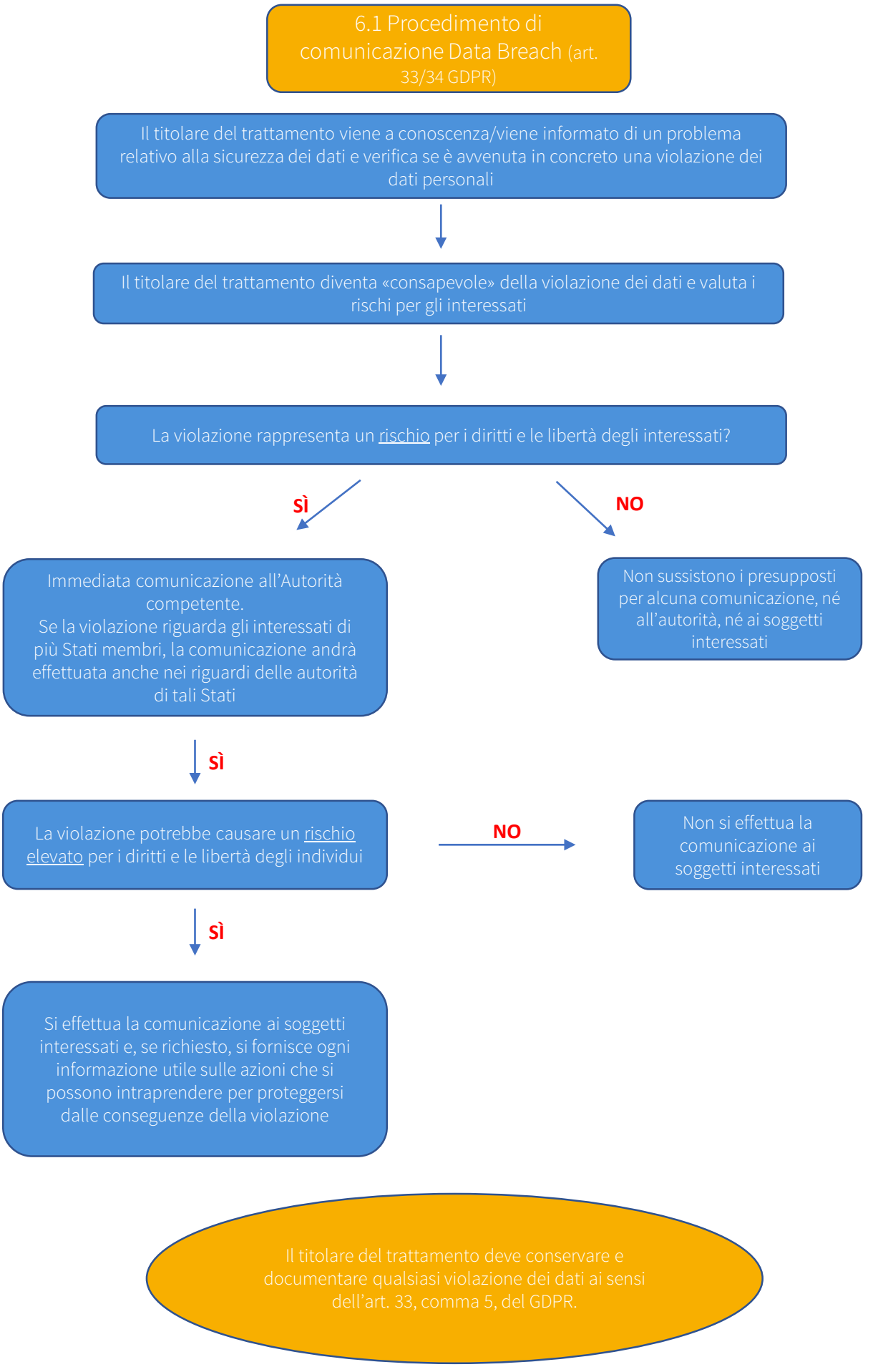
- L´obiettivo della devoluzione di competenze a favore dell´autorità capofila è garantire l´esistenza di uno "**sportello unico**" per i trattamenti transfrontalieri di dati personali.

- L' Autorità capofila coopera con le altre autorità interessate, ed avrà la competenza di emettere decisioni vincolanti per le altre autorità. Nel caso in cui il trattamento incida solo su interessi locali, il principio non si applica e la competenza rimane dell'Autorità del paese del trattamento.

Working Party 29

- Infine, il WP29 ha preso in esame anche i cosiddetti "*borderline cases*", cioè le situazioni in cui è estremamente complicato individuare lo stabilimento principale o il luogo in cui le decisioni relative al trattamento vengono prese. In tali casi, la società dovrà designare lo stabilimento che funge da stabilimento principale e, nel caso in cui questo non sia possibile, sarà compito delle Autorità di controllo procedere all'individuazione dello stesso.

6. LA VIOLAZIONE DEI DATI PERSONALI


6.1 Procedimento di comunicazione Data Breach (art. 33/34 GDPR)
Il titolare del trattamento viene a conoscenza/viene informato di un problema relativo alla sicurezza dei dati e verifica se è avvenuta in concreto una violazione dei dati personali
Il titolare del trattamento diventa «consapevole» della violazione dei dati e valuta i rischi per gli interessati
La violazione rappresenta un rischio per i diritti e le libertà degli interessati?
SÌ
NO
Immediata comunicazione all'Autorità competente.
Se la violazione riguarda gli interessati di più Stati membri, la comunicazione andrà effettuata anche nei riguardi delle autorità di tali Stati
Non sussistono i presupposti per alcuna comunicazione, né all'autorità, né ai soggetti interessati
SÌ
La violazione potrebbe causare un rischio elevato per i diritti e le libertà degli individui
NO
Non si effettua la comunicazione ai soggetti interessati
SÌ
Si effettua la comunicazione ai soggetti interessati e, se richiesto, si fornisce ogni informazione utile sulle azioni che si possono intraprendere per proteggersi dalle conseguenze della violazione
Il titolare del trattamento deve conservare e documentare qualsiasi violazione dei dati ai sensi dell'art. 33, comma 5, del GDPR.

6.2 RESPONSE TEAM - INSPECTION BY THE ITALIAN Data Protection Authority

Country Legal **Primary** Name: Email: Office Tel: Mobile:	 **Back-up** Name: Email: Office Tel: Mobile:
External Lawyer **Primary** Name: Email: Office Tel: Mobile:	 **Back-up** Name: Email: Office Tel: Mobile:
HR Contact **Primary** Name: Email: Office Tel: Mobile:	 **Back-up** Name: Email: Office Tel: Mobile:
IT Contact **Primary** Name: Email: Office Tel: Mobile:	 **Back-up** Name: Email: Office Tel: Mobile:
Cybersecurity **Primary** Name: Email: Office Tel: Mobile:	 **Back-up** Name: Email: Office Tel: Mobile:
Marketing **Primary** Name: Email: Office Tel: Mobile:	 **Back-up** Name: Email: Office Tel: Mobile:
Business contact	

Primary Name: Email: Office Tel: Mobile:	**Back-up** Name: Email: Office Tel: Mobile:
Store contact **Primary** Name: Email: Office Tel: Mobile:	 **Back-up** Name: Email: Office Tel: Mobile:
CSS contact **Primary** Name: Email: Office Tel: Mobile:	 **Back-up** Name: Email: Office Tel: Mobile:
Local DPO (where available) **Primary** Name: Email: Office Tel: Mobile:	

6.3 ESEMPI DI VIOLAZIONE DEI DATI PERSONALI

Esempio	Notifica all'autorità?	Notifica all'interessato?	Commento
1) Un supporto (cd; dvd; chiavetta USB; cassetta) contente un backup di un archivio di dati personali criptati viene rubato.	No.	No.	Fintantochè i dati personali sono crittografati con un algoritmo di ultima generazione, esistono dei backup dei dati in altri supporti, potendo così essere recuperati in breve tempo, non é necessario notificare la violazione. Tuttavia, se venisse compromessa successivamente, la notificazione è richiesta.
2) Un titolare dei dati conserva la documentazione sui dati personali avvalendosi di una società fornitrice di servizi online. A seguito di un attacco hacker a tale società, i dati personali dei soggetti sono stati estrapolati. Il titolare dei dati ha clienti di uno Stato membro dell'Unione europea.	Sì, deve essere data comunicazione all'autorità se ci sono probabili conseguenze verso gli interessati.	Sì, viene data comunicazione agli interessati secondo la natura dei dati personali coinvolti e se la gravità delle probabili conseguenze è alta.	
3) Una breve interruzione dell'alimentazione del call center del titolare del trattamento, che comporta l'impossibilità dei clienti di chiamare il titolare del trattamento ed accedere ai propri dati.	No.	No.	Non c'è una violazione da notificare, ma siamo ancora sotto la violazione da documentarre di cui all'art. 33, c. 5. L'appropriato registro dovrebbe essere tenuto dal responsabile dei dati.
4) Un titolare dei dati subisce un attacco malware che causa la crittografia di tutti i dati personali. Non sono disponibili copie di backup, né il ristoro dei dati personali. A seguito di opportune verifiche, diventa chiaro che la sola e unica funzione del malware era quella di criptare i dati, e che non c'era alcun ulteriore malware presente nel sistema.	Sì, deve essere data comunicazione all'autorità se ci sono probabili conseguenze verso gli interessati, come per esempio la mancata disponibilità dei dati.	Sì, viene data comunicazione agli interessati, secondo ì la natura dei dati personali violati, il possibile effetto della mancata disponibilità dei dati e le altre probabili conseguenze.	Se ci fosse stata una copia di backup disponibile, e i dati potessero essere ripristinati entro un termine accettabile, non ci sarebbe bisogno di dare comunicazione della violazione all'autorità né agli interessati, in quanto non ci sarebbe stata alcuna perdita permanente della disponibilità dei dati o della loro confidenzialità.

			Comunque, se l'autorità competente fosse stata avvertita dell'incidente in altri modi, la stessa avrebbe potuto considerare unìindagine per valutare la conformità con tutti i requisiti di sicurezza di cui all'art. 32.
5) Un interessato denuncia al call center di una banca una violazione dei dati. La persona ha ricevuto infatti il bilancio mensile di un altro cliente della banca. Il titolare dei dati avvia quindi una breve investigazione (completata entro 24 ore) e stabilisce con ragionevole certezza che è avvenuta una violazione dei dati personali, la quale potrebbe avere natura sistematica e intaccare pertanto i dati di altri soggetti.	Sì, deve essere data comunicazione all'autorità.	Sono informati del fatto solo gli interessati coinvolti nella violazione, qualora ci sia alto rischio di violazione dei dati e sia chiaro che gli altri interessati non siano stati coinvolti.	Se, a seguito di ulteriori indagini, è verificato che più di un soggetto è stato coinvolto, deve essere effettuato un aggiornamento all'autorità competente. Il responsabile del trattamento intraprende gli step sucessivi per notificare agli altri soggetti l'eventuale alto rischio nei loro confronti.
6) Un titolare dei dati lavora in uno store online e ha clienti in più Stati membri. Lo store subisce un attacco da parte di un hacker, il quale procede poi alla pubblicazione in internet di usernames, passwords e storico degli ordini.	Sì, se la violazione coinvolge più Stati membri, deve essere data comunicazione all'autorità.	Sì, viene data comunicazione agli interessati in quanto il fatto potrebbe causare un alto rischio di violazione dei dati.	Il responsabile del trattamento dovrebbe attivarsi, ad es. resettando le password degli account violati, o adottando altre misure per mitigare il rischio. Il responsabile del trattamento dovrebbe anche considerare ogni altra comunicazione obbligatoria, ad es. secondo la Direttiva NIS in quanto provider di servizi.
7) Un'azienda che svolge servizi di hosting di siti internet agisce come titolare dei dati e identifica un errore nel codice che controlla l'autorizzazione degli utenti. L'effetto dell'errore comporta che ogni utente può accedere ai dettagli dell'account di ogni altro utente.	Come titolare del trattamento dei dati, la società di hosting deve dare comunicazione ai clienti coinvolti (i responsabili del trattamento) senza ritardo. Presupponendo che la società di hosting abbia condotto un'autonoma indagine, i responsabili del trattamento dovrebbero ragionevolmente essere	Se non è probabile un alto rischio per i dati degli interessati, non c'è bisogno che vengano informati del fatto.	La società di hosting (titolare del trattamento) deve considerare ogni altra comunicazione obbligatoria, ad es. secondo la Direttiva NIS in quanto provider di servizi. Se non vi è prova che questa vulnerabilità del sistema venga sfruttata nei confronti dei responsabili del trattamento, una violazione notificabile

	rassicurati dal fatto che conosceranno la concreta portata della violazione e i soggetti realmente coinvolti. Inoltre, è probabile che siano considerati edotti del fatto dal momento della comunicazione ricevuta dalla società di hosting (titolare dei dati). Il responsabile del trattamento dovrà poi darne comunicazione all'autorità.		potrebbe non essersi verificata, ma è comunque presumibile che tale fatto venga opportunamente registrato o sia soggetto alla non-compliance di cui all'art. 32.
8) I registri medici di un ospedale sono indisponibili per un periodo di 30 ore a causa di un cyber attacco.	Sì, l'ospedale è obbligato a dare comunicazione all'autorità in quanto potrebbe verificarsi un alto rischio di violazione di dati personali relativi allo stato di buona salute dei pazienti e quindi della loro privacy.	Sì, viene data comunicazione agli interessati.	
9) I dati personali di un gran numero di studenti sono stati inviati erroneamente ad una mailing list con più di mille destinatari.	Sì, deve essere data comunicazione all'autorità.	Sì, viene data comunicazione agli interessati a seconda dello scopo e del tipo dei dati personali coinvolti e della gravità delle possibili conseguenze.	
10) Una e-mail di marketing a risposta diretta è inviata alla lista di destinatari lasciandoli in "cc", consentendo a ciascun destinatario di visualizzare l'indirizzo di posta elettronica di altri destinatari.	Sì, notificare l'autorità competente potrebbe essere obbligatorio se un grande numero di soggetti sono coinvolti, se sono stati rivelati dati senibili (per es. una mailing list di un psicoterapeuta) o se altri fattori espongono i dati ad un alto rischio di violazione (per es. la mail contiene le password).	Sì, viene data comunicazione agli interessati a seconda dello scopo e del tipo dei dati personali coinvolti e della gravità delle possibili conseguenze.	La comunicazione potrebbe non essere necessaria se non si è verificata alcuna diffusione di dati sensibili e se sono stati rivelati solo una minoranza di indirizzi e-mail.
11) Un provider di servizi telefonici è stato vittima di una violazione di dati personali, essendo stata sfruttata una vulnerabilità nel sistema che ha consentito l'accesso, con successiva copia, alle credenziali di autenticazione (user-id e password) di circa 5000 clienti. Per circa 400 clienti risultava un avvenuto accesso all'area personale	Sì.	Sì, a tutti i circa 5000 utenti che hanno subìto la violazione.	La sola acquisizione di credenziali di accesso è da ritenere già di per sé fonte di potenziale pregiudizio per gli interessati, indipendentemente dal fatto che ne consegua un effettivo utilizzo per accedere a specifiche aree riservate. Questo in considerazione della probabilità che le

loro dedicata contestualmente al periodo dell'incidente (Provvedimento Autorità Garante per la Privacy 2017 [6431926])			medesime credenziali possano essere utilizzate per accedere a diversi portali web, atteso che la user-id è costituita dal numero telefonico dell'utente.
12) Un'azienda combina il data mining, l'intermediazione dei dati e l'analisi dei dati con la comunicazione strategica per le campagne elettorali, utilizzando impropriamente i dati personali di circa 200 mila utenti italiani (e milioni di utenti a liivello mondiale) iscritti a un social network. (Caso Facebook-Cambridge Analytica, 2018)	Sì.	Sì, a tutti gli utenti i cui dati sono stati violati	Chi ha subito un danno ne sarà consapevole e potrà chiedere al social maggiori informazioni su come sono state gestiti propri dati.

Primo caso di Data Breach da quando è in vigore il GDPR:

British Airways è stata vittima di un attacco informatico al proprio sito e alla propria app: sono stati rubati i dati dei clienti (circa 380.000) che, tramite essi, hanno effettuato prenotazioni e modifiche nel periodo tra il 21 agosto e il 5 settembre 2018. Fra i dati oggetto di furto sono inclusi dati personali (quali nomi, indirizzo di fatturazione, indirizzo email) e finanziari (dati del conto bancario), ma non i dati di viaggio o del passaporto. Si tratta del primo caso di data breach da quando è in vigore il Regolamento Europeo 2016/679 (GDPR) e British Airways, in conformità all'articolo 33 GDPR, ha comunicato la violazione all'Autorità di controllo competente entro le 72 ore da quando ne è venuta a conoscenza. L'ICO ha infatti emesso, il 7 settembre 2018, un breve comunicato al riguardo, in cui afferma di aver ricevuto notifica del data breach e che indagherà (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-statement-in-response-to-british-airways-breach-announcement/).

Inoltre, ai sensi dell'articolo 34 GDPR, British Airways ha comunicato, con linguaggio semplice e chiaro, l'avvenuta violazione agli interessati, mediante la pubblicazione di informazioni sul suo sito (https://www.britishairways.com/it-it/information/incident/data-theft/latest-information). Viene spiegato chi possano essere gli interessati coinvolti, che verranno comunque contattati con la finalità di porgere le proprie scuse e di aggiornali. Si raccomanda loro di contattare la propria banca o fornitore di carta di credito, in modo da seguire i loro consigli, e di stare attenti ad eventuali tentativi di phishing. British Airways si impegna inoltre al rimborso per qualsiasi attività fraudolenta risultato diretto del data breach e ad un servizio di monitoraggio del rating del credito per 12 mesi a tutti i clienti. In aggiunta, sono stati pubblicati annunci di scuse sui quotidiani e il CEO ha rilasciato interviste al riguardo.

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-statement-in-response-to-british-airways-breach-announcement/

http://www.affaritaliani.it/cronache/british-airways-hackerata-confermata-la-violazione-dati-di-380000-clienti-558846.html

6.4 COMPARAZIONE DEGLI ILLECITI PENALI

Art. 167 cod. privacy (trattamento illecito di dati)
Condotta ex D.lgs. 101/2018: Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

D.lgs. 196/2003 (nota 1)	Schema D.lgs. 10/5/2018	D.lgs. 101/2018 (GU: 4/9/2018)
art. 123 c. pr. (violazione prescrizioni relative ai dati relativi al traffico)	art. 123 c. pr. (violazione prescrizioni relative ai dati relativi al traffico)	art. 123 c. pr. (violazione prescrizioni relative ai dati relativi al traffico)
art. 126 c. pr. (violazione prescrizioni relative ai dati relativi l'ubicazione)	art. 126 c. pr. (violazione prescrizioni relative ai dati relativi l'ubicazione)	art. 126 c. pr. (violazione prescrizioni relative ai dati relativi l'ubicazione)
art. 129 c. pr. (violazione provvedimento Garante elenco contraenti)	art. 129 c. pr. (violazione provvedimento Garante elenco contraenti)	art. 129 c. pr. (violazione provvedimento Garante elenco contraenti)
art. 130 c. pr (violazione prescrizioni relative alla comunicazioni indesiderate)	art. 130 c. pr (violazione prescrizioni relative alla comunicazioni indesiderate)	art. 130 c. pr (violazione prescrizioni relative alla comunicazioni indesiderate)
	art. 2-sexies (violazioni afferenti il trattamento di particolari categorie di dati effettuato per motivi di interesse pubblico rilevante)	art. 2-sexies (violazioni afferenti il trattamento di particolari categorie di dati effettuato per motivi di interesse pubblico rilevante)
		art. 2-septies (Misure di garanzia per il trattamento di dati genetici, biometrici e relativi alla salute)
	art. 2-octies (violazioni afferenti il trattamento di dati relativi condanne penali e reati)	art. 2-octies (violazioni afferenti il trattamento di dati relativi condanne penali e reati)
	art. 2-quaterdecies (violazione di prescrizioni generali del Garante per il trattamento di dati per scopi int. Pubb.)	
		art. 2-quinquiesdecies (trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico)
	comma 3° (trasferimento dati vs paese terzo o organizzazione internazionale in violazione degli artt. 45, 46 o 49 GDPR)	comma 3° (trasferimento dati vs paese terzo o organizzazione internazionale in violazione degli artt. 45, 46 o 49 GDPR)

art. 167-bis cod. privacy (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)
Condotta ex D.lgs. 101/2018: Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione. 3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167

D.lgs. 196/2003	Schema D.lgs. 10/5/2018	D.lgs. 101/2018 (GU: 4/9/2018)
NON APPLICABILE (NORMA NON PREVISTA)	art. 2-ter (base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri)	art. 2-ter (base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri)
	art. 2-sexies (violazioni afferenti il trattamento di particolari categorie di dati effettuato per motivi di interesse pubblico rilevante)	art. 2-sexies (violazioni afferenti il trattamento di particolari categorie di dati effettuato per motivi di interesse pubblico rilevante)
	art. 2-octies (violazioni afferenti il trattamento di dati relativi condanne penali e reati)	art. 2-octies (violazioni afferenti il trattamento di dati relativi condanne penali e reati)

art. 167-ter cod. privacy (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala)
Condotta ex D.lgs. 101/2018: Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.

D.lgs. 196/2003	Schema D.lgs. 10/5/2018	D.lgs. 101/2018 (GU: 4/9/2018)
NON APPLICABILE (NORMA NON PREVISTA)	PREVISTA	PREVISTA

art. 168 cod. privacy (Falsità nelle dichiarazioni al Garante e interruzione dei compiti o dell'esercizio dei poteri del Garante)
Condotta ex D.lgs. 101/2018: Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni. 2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti

D.lgs. 196/2003	Schema D.lgs. 10/5/2018	D.lgs. 101/2018 (GU: 4/9/2018)

art. 170 cod. privacy (Inosservanza di provvedimenti del Garante)
Condotta ex D.lgs. 101/2018: Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 è punito con la reclusione da tre mesi a due anni (**nota 2**)

D.lgs. 196/2003	Schema D.lgs. 10/5/2018	D.lgs. 101/2018 (GU: 4/9/2018)
PREVISTA	*NON APPLICABILE (NORMA NON PREVISTA)*	PREVISTA

art. 171 cod. privacy (Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori)
Condotta ex D.lgs. 101/2018: La violazione delle disposizioni di cui agli *articoli 4*, comma 1, e *8 della legge 20 maggio 1970, n. 300*, è punita con le sanzioni di cui all'articolo 38 della medesima legge.

D.lgs. 196/2003	Schema D.lgs. 10/5/2018	D.lgs. 101/2018 (GU: 4/9/2018)
Art. 4, comma 1 legge n. 300/1970 (Impianti audiovisivi e altri strumenti di controllo)	Art. 4, comma 1 legge n. 300/1970 (Impianti audiovisivi e altri strumenti di controllo)	Art. 4, comma 1 legge n. 300/1970 (Impianti audiovisivi e altri strumenti di controllo)
Art. 4, comma 2 legge n. 300/1970 (Impianti audiovisivi e altri strumenti di controllo)	Art. 4, comma 2 legge n. 300/1970 (Impianti audiovisivi e altri strumenti di controllo)	
[*Art. 113 c. pr. (Raccolta di dati e pertinenza: rinvio diretto ad Art. 8 legge n. 300/1970)*]	Art. 8 legge n. 300/1970 (Divieto di indagini sulle opinioni)	Art. 8 legge n. 300/1970 (Divieto di indagini sulle opinioni)
Art. 38, legge n. 300/1970 (Disposizioni penali)	Art. 38, legge n. 300/1970 (Disposizioni penali)	Art. 38, legge n. 300/1970 (Disposizioni penali)

art. 172 cod. privacy (Pene accessorie)
Condotta ex D.lgs. 101/2018: La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza, ai sensi dell'articolo 36, secondo e terzo comma, del codice penale

D.lgs. 196/2003	Schema D.lgs. 10/5/2018	D.lgs. 101/2018 (GU: 4/9/2018)
	Art. 36, secondo e terzo comma, del codice penale	Art. 36, secondo e terzo comma, del codice penale

Note esplicative e legenda

nota 1 per maggiore leggibilità del foglio è stata omessa la citazione degli articoli 17, 20, 21, 22, commi 8 e 11, 25, 27 e 45, richiamati nel testo dell'art. 167 cod. privacy versione D.lgs. 196/03. Tali articoli non sono stati richiamati nello schema di D.lgs. 10/5/2018 e nel D.lgs. 101/2018

nota 2 il testo dell'art. 170 è stato in parte riformulato dal D.lgs. 101/18, rispetto alla versione del D.lgs. 196/2003, di cui conserva identica la rubrica

Legenda:

(i) in caratteri rossi sono evidenziate le modifiche apportate al testo delle norme considerate dal D.lgs. 101/2018, rispetto alla versione contemplata nello schema di D.lgs. del 10/5/18.

(ii) Gli articoli del codice privacy citati (nel foglio anche solo nel "cod. privacy" o "c. pr") si riferiscono al contenuto, a seconda della colonna dove sono indicati, posto dall'originario D.lgs. 196/2003 oppure dallo schema di D.lgs. 10/5/2018 o dal D.lgs. 101/2018.

(iii) Gli articoli che non sono seguiti da alcun riferimento a "codice privacy" si riferiscono all' provvedimento normativo relativo alla colonna di appartenenza (e quindi, alternativamente, a seconda del caso, lo schema di D.lgs. 10/5/2018 oppure il D.lgs. 101/2018