Cerved Group S.p.A.

POLICY

Generale in materia di

Trattamento di Dati Personali

Approvata dal Consiglio di Amministrazione in data 23 dicembre 2019

Indice

1 Scopo e campo di applicazione

1.1 SCOPO

Il presente documento ("**Politica**" o "**Policy**") ha l'obiettivo di definire gli impegni assunti e le politiche attuate da Cerved Group S.p.A. ("**Cerved**") e delle società appartenenti al relativo gruppo ("**Gruppo Cerved**"[1]) in materia di protezione dei Dati Personali, in relazione all'organizzazione societaria e ai ruoli rilevanti in funzione dell'applicazione della normativa vigente sulla privacy, nonché alle procedure, disposizioni e misure adottate per assicurare la conformità a tale normativa.

La Politica, per la cui redazione e revisione sono state coinvolte tutte le strutture aziendali interessate, è approvata dal Consiglio di Amministrazione di Cerved.

La Politica sarà riesaminata e, se del caso, rivista periodicamente anche in relazione ad aggiornamenti delle normative di riferimento e della prassi interpretativa del Comitato Europeo Protezione Dati (*European Data Protection Board* – "**EDPB**") e del Garante Protezione Dati Personali ("**Garante**"), nonché alle evoluzioni dell'organizzazione ed attività societarie, dei progetti e processi aziendali e delle piattaforme ed applicazioni informatiche in uso.

La Politica è pubblicata sul sito internet di Cerved (www.cerved.com), nonché comunicata e resa disponibile a tutto il personale interessato mediante *l'intranet* aziendale e la piattaforma *Workplace*, assieme alle indicazioni operative e documentazioni adottate internamente.

Cerved si impegna ad informare tempestivamente gli interessati in caso di modifiche o variazioni della presente Politica, provvedendo senza ritardo alla pubblicazione dei relativi aggiornamenti sul relativo sito web.

1.2 CAMPO DI APPLICAZIONE

La procedura si applica a tutte le società del Gruppo Cerved.

1.3 DESTINATARI

La presente Politica si applica a tutte le attività di Trattamento di Dati Personali svolte nell'ambito del Gruppo Cerved, da tutti gli organi, funzioni e reparti aziendali e dalle persone autorizzate al Trattamento, nonché alle attività di Trattamento effettuate per conto del Gruppo Cerved dai soggetti che agiscono in qualità di responsabili di tale Trattamento.

[1] Situazione aggiornata (Struttura del Gruppo) consultabile al link: https://company.cerved.com/it/struttura-del-gruppo

2 Riferimenti

2.1 LE NORME DI RIFERIMENTO

Come noto, 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 ("**GDPR**" o "**Regolamento**"), applicabile dal 25 maggio 2018, ha abrogato la precedente Direttiva 95/46/CE del 24 ottobre 1995, rendendo conseguentemente disapplicabili anche le normative nazionali emanate in applicazione di tale Direttiva, almeno nelle parti che risultano incompatibili ed in contrasto con le disposizioni del medesimo GDPR.

Con il d.lgs. 10 agosto 2018 n. 101, entrato in vigore il 19 settembre 2018, si è recentemente provveduto all'adeguamento alle disposizioni del GDPR della normativa italiana sulla privacy, costituita essenzialmente dal d.lgs. n. 196/2003 - Codice in materia di protezione dei Dati Personali ("**Codice Privacy**"), che è stato oggetto di una vera e propria riforma da parte del d.lgs. 101/2018 con conseguente abrogazione, modificazione ed integrazione di diverse disposizioni.

Allo stato, la protezione dei Dati Personali risulta, pertanto, disciplinata in Italia dal GDPR e dal Codice privacy, così come modificato dal d.lgs. 101/2018, nonché dal Codice di condotta per il Trattamento dei Dati Personali in materia di informazioni commerciali, presentato da Ancic e approvato dal Garante con provvedimento del 12 giugno 2019, con efficacia subordinata al completamento della fase di accreditamento dell'organismo di monitoraggio da parte della medesima Autorità, dai provvedimenti generali e linee guida del Garante per la protezione dei Dati Personali, nonché dai provvedimenti e linee guida del precedente Gruppo di Lavoro ex art. 29 della Dir. 95/46/CE (**WP29**), sostituito ora dall'EDPB, che forniscono indirizzi, indicazioni, raccomandazioni e chiarimenti applicativi in merito agli adempimenti introdotti dal GDPR, di cui si è ampiamente tenuto conto nella predisposizione della presente Policy.

In allegato sono riportati un glossario con le principali definizioni utilizzate nel presente documento, in linea con le previsioni normative, nonché due appendici concernenti i principali adempimenti previsti e novità introdotte dal GDPR che Cerved e le società del Gruppo Cerved si impegnano a rispettare al fine di garantire la conformità delle relative attività al medesimo Regolamento.

3 Organizzazione dei ruoli, compiti e responsabilità in funzione della protezione dei Dati Personali

Cerved, quale Titolare del Trattamento, ha definito ruoli e responsabilità che garantiscono l'indirizzo, il governo, l'esecuzione e il controllo del nuovo modello organizzativo per la protezione dei Dati Personali.

3.1 ORGANI, FUNZIONI, AREE E *BUSINESS UNIT*

3.1.1 Consiglio di Amministrazione

Il Consiglio di Amministrazione, quale organo di vertice di Cerved, ha delegato all'Amministratore Delegato i principali poteri relativi all'organizzazione, gestione e controllo degli adempimenti privacy procedendo all'attribuzione ai responsabili *pro tempore* di alcune aree aziendali di diretto riporto al vertice societario, nei limiti dei poteri agli stessi già assegnati, della qualifica di "*Delegato privacy*", conferendo ai medesimi specifiche deleghe di funzioni riguardo all'applicazione della normativa privacy, disciplinando i relativi compiti e responsabilità al fine di assicurare la corretta gestione delle attività di Trattamento dei Dati Personali svolte nelle rispettive aree di competenza e l'adempimento degli obblighi previsti dal GDPR.

3.1.2 Delegati Privacy

I Delegati Privacy, individuati come sopra, ricevono apposite informazioni ed adeguati aggiornamenti formativi in materia di protezione dei dati e hanno la possibilità di individuare, all'interno della propria struttura, uno o più referenti o collaboratori (c.d. "*Privacy Contact*": v.- infra 3.1.3) che li supportino nelle attività da svolgere in funzione dell'applicazione delle norme privacy. Ciascun Delegato Privacy sarà chiamato a svolgere funzioni di direzione, coordinamento e controllo delle attività di Trattamento dei Dati Personali svolte nell'ambito della relativa area di competenza e dei correlati adempimenti previsti dal GDPR effettuati nell'ambito delle attività di pertinenza di tale area, ivi incluso il potere di supervisionare l'attuazione dei provvedimenti e delle misure tecniche e organizzative necessarie a norma degli articoli 24 e 32 del GDPR, al fine di permettere al Titolare del Trattamento dei dati di garantire ed essere in grado di dimostrare che il Trattamento dei Dati Personali è effettuato conformemente alla normativa vigente, facendosi parte attiva ai fini dell'effettivo utilizzo e del rispetto delle policy, procedure e linee guida adottate dal Gruppo Cerved ai fini dell'adeguamento al GDPR.

3.1.3 Privacy Contact

Il Gruppo Cerved ha previsto l'attribuzione ad alcune persone autorizzate al Trattamento del ruolo di Privacy Contact. I Privacy Contact partecipano agli interventi di formazione specifica sulla

normativa in materia di Trattamento dei Dati Personali e sono tenuti a svolgere un ruolo di garanzia al fine di determinare il rispetto del principio di *accountability*, cooperando attivamente affinché siano concretamente rispettate e attuate le procedure e le linee guida di cui si sono dotate le società del Gruppo Cerved ai fini di adeguamento al GDPR (con particolare riferimento alla tenuta del registro dei trattamenti ex art. 30 del GDPR e dello svolgimento delle correlate analisi dei rischi, alla "*Procedura di Valutazione di Impatto sulla Protezione dei Dati*", alle "*Linee Guida Data Protection by Design e by Default*" e alla "*Procedura sulla Gestione delle Violazioni dei Dati Personali"*).

I Privacy Contact sono responsabili per l'adozione e il rispetto da parte delle persone autorizzate, che risultano sottoposte al loro coordinamento o per in relazione alle quali vengano legittimati dai Delegati Privacy di riferimento, le opportune misure di sicurezza previste dalla normativa in materia di Trattamento dei Dati Personali per ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di Trattamento non consentito o non conforme alle finalità della raccolta. A tale scopo dovrà vigilare anche sul corretto svolgimento delle attività di Trattamento eseguite da tutti gli autorizzati appartenenti alla sua area di competenza secondo quanto definito all'interno dell'organigramma aziendale e assicurarsi che ricevano ed eseguano opportune istruzioni sulle modalità pratiche di Trattamento dei dati.

3.1.4 Data Protection Officer (DPO)

Come detto, la figura a cui sarà assegnato il ruolo di Responsabile della Protezione dei Dati (di seguito, "**DPO**") deve essere dotata di autonomia ed indipendenza ed essere in grado di dare consulenza specialistica in materia di protezione dati alle strutture (*business unit*) del Gruppo Cerved e, nel contempo, svolgere attività di controllo, in genere, di secondo livello sulle procedure, misure e documentazioni dalle stesse adottate per verificarne la conformità al GDPR, dovendo poi fornire indicazioni e raccomandazioni in proposito al competente organo di vertice della relativa società del Gruppo Cerved (riferendo direttamente all'AD o ad altro soggetto a ciò delegato da quest'ultimo o dal CdA, anche mediante relazioni periodiche, salvo casi urgenti da segnalare senza ritardo).

Cerved, quale capogruppo, ha valutato la necessità di individuare un DPO, in base a quanto previsto dal Considerando 97 e dall'art. 37 del GDPR, dalle Linee Guida del WP29 per la protezione dati sui responsabili della protezione dati[2] e dalle Faq in ambito privato del Garante[3] e ha ritenuto di avvalersi della facoltà, prevista dall'art. 37, paragrafo 2, del Regolamento, di

[2] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
[3] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793

procedere alla nomina condivisa di uno stesso DPO per tutte le società appartenenti al Gruppo Cerved, ad eccezione delle società estere del Gruppo Cerved che hanno provveduto a designare dei DPO locali.

In particolare, il Gruppo Cerved ha ritenuto di affidare la funzione di DPO all'esterno della propria organizzazione, all'esito del processo di selezione teso all'individuazione di un candidato in possesso dei requisiti richiesti dal GDPR ai fini dell'espletamento dell'incarico di DPO per l'intero gruppo imprenditoriale, verificando che fosse in possesso del livello di conoscenza specialistica e delle competenze richieste dall'art. 37, par. 5 del GDPR e che, in conformità a quanto previsto ai sensi dall'art. 38 par. 6 del GDPR, non si trovasse in situazioni di conflitto di interesse in relazione ad eventuali altri compiti e funzioni che può svolgere per il Gruppo Cerved medesimo. Pertanto le società del Gruppo Cerved hanno designato il DPO del Gruppo Cerved con delibera del Consiglio di Amministrazione.

Il Gruppo Cerved ha, altresì, individuato nei professionisti della direzione legale di Cerved, esperti in materia di protezione dei Dati Personali, figure che possano tra le altre cose facilitare il coordinamento delle risorse interne con il DPO designato, al fine di mettere quest'ultimo nelle condizioni di assolvere più agevolmente i propri compiti, secondo quanto previsto dall'art. 38, par. 2, del GDPR.

I dati di contatto del DPO sono, inoltre, stati comunicati al Garante e pubblicati sul sito internet istituzionale tramite le informative privacy.

3.1.5 Internal Audit

L'*internal Audit*:

- verifica, sia in via continuativa sia in relazione a specifiche necessità e nel rispetto degli standard internazionali, l'operatività e l'idoneità del sistema di controllo interno e di gestione dei rischi, attraverso un piano di audit, approvato dal CdA, basato su un processo strutturato di analisi e prioritizzazione dei principali rischi;
- verifica il corretto ed efficace funzionamento dei modelli di gestione del rischio adottati dall'azienda, incluso il rischio di *compliance*, con lo scopo di assicurare che quanto adottato consenta al management un'efficace gestione dei rischi, sia dal punto di vista metodologico che strumentale.

In tale contesto, nel piano di audit delle società del Gruppo Cerved, è previsto uno specifico audit "*Verifica di efficacia dei controlli in ambito compliance "GDPR*". È altresì prevista, nel continuo, una attività di verifica del "*Sistema di Gestione della Sicurezza delle Informazioni*" del Gruppo

Cerved, svolta in conformità allo standard ISO 27001:2017, volta a verificare l'adeguatezza delle misure di sicurezza tecnico organizzative adottate.

Inoltre, all'interno degli specifici "*audit di processo*", possono essere previste verifiche attinenti la corretta applicazione delle prescrizioni GDPR (sia relativamente alla normativa esterna, che interna).

Le attività collegate (direttamente o indirettamente) all'ambito GDPR, vengono svolte con la collaborazione/in coordinamento con il DPO e i Privacy Executive del Gruppo Cerved.

3.1.6 IT

La rispettiva area IT di ciascuna società del Gruppo Cerved, unitamente al Delegato Privacy che svolge funzioni di direzione, coordinamento e controllo delle attività di Trattamento dei Dati Personali svolte nell'ambito della suddetta area di competenza, è tenuta ad effettuare, con riferimento ai sistemi informatici e ai servizi IT della rispettiva società del Gruppo Cerved, l'analisi dei rischi per la sicurezza dei dati al fine di individuare le misure di sicurezza da implementare, valutandone l'efficacia, la gestione e notifica di un *data breach*. Fornisce inoltre supporto per gli aspetti tecnici/tecnologici alla procedura di valutazione d'impatto (c.d. "*DPIA*") e supporta il DPO sulle tematiche informatiche, cura per conto del Titolare la gestione di obblighi ed attività più tecniche inerenti l'attuazione della disciplina in materia di protezione dei Dati Personali, anche fornendo in proposito alle aree aziendali supporto specialistico sia consultivo che di controllo, con particolare riferimento alla supervisione e coordinamento delle attività di attuazione delle policy aziendali e del Gruppo Cerved in materia di sicurezza dei dati e dei sistemi, all'analisi e valutazione dei rischi connessi, sotto il profilo tecnico o tecnologico, alle attività di Trattamento dei Dati Personali, all'aggiornamento e presidio delle infrastrutture e misure tecnologiche rispetto alle normative privacy, nonché alla gestione dei *data breach* sopra descritti. A tale area sono attribuite, oltre alle responsabilità concernenti la cura dei trattamenti di Dati Personali comunque acquisiti, registrati, generati e/o conservati nell'ambito dei sistemi informativi dalla stessa gestiti, anche specifiche funzioni attinenti agli aspetti relativi alla valutazione, pianificazione, adozione e controllo nel Gruppo Cerved delle misure tecniche e di sicurezza dei suddetti dati e sistemi per assicurare la conformità agli standard previsti dal GDPR, sulla base anche delle *policies* di gruppo, nonché il ruolo di "*focal point*" per quanto riguarda la gestione e notificazione di eventuali *data breach*, ove tali violazioni riguardino i sistemi informatici e telematici del Gruppo Cerved, su cui, ove ritenuto necessario, potrà essere richiesto tempestivamente anche il supporto consultivo del DPO.

3.1.7 Risorse umane

All'area Risorse umane sono delegate le funzioni inerenti l'osservanza delle disposizioni del GDPR e delle norme nazionali in relazione al Trattamento dei Dati Personali dei dipendenti e lavoratori assimilati nel Gruppo Cerved, possono essere assegnati ulteriori compiti riguardanti, in generale, anche l'individuazione, assieme ai responsabili delle aree cui sono assegnate, dei dipendenti/collaboratori autorizzati al Trattamento dei Dati Personali e degli ambiti di Trattamento loro consentiti, la definizione delle garanzie di riservatezza e delle documentate istruzioni in materia, nonché la realizzazione delle attività formative in base alle esigenze delle strutture aziendali.

3.1.8 Persone autorizzate ai Trattamenti

Il Gruppo Cerved provvede all'individuazione del personale autorizzato al Trattamento di Dati Personali nell'ambito dell'area, unità od ufficio di appartenenza, che opera sotto la direzione e il controllo del relativo responsabile o Delegato Privacy e che è tenuto ad attenersi alle istruzioni ricevute nel rispetto della normativa privacy, nonché alle "*Linee guida sulle Persone Autorizzate al Trattamento dei Dati Personali"*, che riportano i ruoli, gli obblighi e le istruzioni relativi alle Persone autorizzate al Trattamento dei Dati Personali dal Gruppo Cerved.

Si prevede specificamente che, all'atto di ingresso nella, ogni Persona autorizzata riceva per la relativa sottoscrizione l'autorizzazione al Trattamento di Dati Personali, che contiene istruzioni specifiche con riferimento ai trattamenti svolti per conto del Gruppo Cerved e attraverso la quale la Persona autorizzata assume un obbligo di riservatezza che perdurerà ben oltre la cessione del rapporto lavorativo o di collaborazione. Unitamente all'autorizzazione al Trattamento di Dati Personali, la Persona autorizzata riceve la "*Policy sull'utilizzo degli strumenti IT"*, disponibile in ogni momento sulla *intranet*, che ricomprende istruzioni riferibili alla gestione delle credenziali affidate, all'uso della posta elettronica, delle rete e degli strumenti aziendali, nonché la "*Procedura per la gestione dei Data Breach"*.

Infine, il Gruppo Cerved promuove annualmente corsi di formazione interni con esperti del settore volti a sensibilizzare le persone autorizzate sul tema della privacy.

3.1.9 Amministratori di sistema

Deve essere considerato amministratore di sistema chiunque, in maniera non occasionale, si occupa della gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di Dati Personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi "*ERP*" (*Enterprise Resource Planning*) utilizzati in grandi aziende e

organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire, anche accidentalmente, sui Dati Personali ("**Amministratori di Sistema**").

Il Gruppo Cerved attribuisce le funzioni di Amministratore di Sistema a soggetti che garantiscano esperienza, capacità e affidabilità previa designazione effettuata individualmente e registrata e conservata in un elenco che reca i nominativi degli Amministratori di Sistema. L'operato di tali soggetti è oggetto di verifica almeno annuale da parte del Titolare del Trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei Dati Personali previste dalle norme vigenti. Inoltre si prevede che vengano adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di.

3.1.10 Responsabili del Trattamento

Il Gruppo Cerved ricorre unicamente a Responsabili che offrano garanzie sufficienti di messa in atto di misure tecniche e organizzative adeguate rispetto ai trattamenti effettuati per suo conto, che siano in grado di soddisfare i requisiti del GDPR e che garantiscano la tutela dei diritti dell'Interessato.

I Trattamenti effettuati dal Responsabile sono disciplinati da specifici contratti che vincolano il Responsabile al Titolare del Trattamento e che definiscono, tra l'altro, 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 Responsabile e del Titolare del Trattamento.

3.1.11 Servizi forniti dal Gruppo Cerved in qualità di Responsabile del Trattamento

Per l'erogazione di determinati servizi, Cerved e/o le altre società del Gruppo Cerved possono effettuare il Trattamento di Dati Personali per conto di altre società del Gruppo Cerved (c.d. *shared services*) e/o soprattutto dei clienti che, quali Titolari, attribuiscono alla stessa società del Gruppo Cerved il ruolo e gli obblighi di Responsabile del Trattamento.

I Trattamenti di Dati Personali effettuati dalle società del Gruppo Cerved, in qualità di Responsabile del Trattamento, connessi all'erogazione dei servizi (es.: informativi, valutativi, di recupero crediti, ecc.), sono disciplinati da appositi contratti ed accordi sul Trattamento dei Dati Personali sottoscritti tra le società del Gruppo Cerved e/o con i clienti ai sensi dell'art. 28 del GDPR e sono monitorati dalle società, aree e funzioni che instaurano e gestiscono i rapporti contrattuali con i medesimi clienti (tramite i rispettivi Delegati privacy e Privacy Contact), al fine dell'attivazione delle conseguenti procedure e misure previste dal GDPR, tra cui la valutazione del rispetto dei requisiti di *privacy by design/default*, l'integrazione del registro dei trattamenti della

società del Gruppo Cerved quale Responsabile, l'adozione di adeguate misure di sicurezza, l'avvio della procedura di DPIA, ecc.

3.2 Procedure e disposizioni adottate per la protezione dei dati personali

Il Gruppo Cerved ha definito una serie di misure organizzative e tecniche interne volte a garantire, ed essere in grado di dimostrare secondo il principio dell'*accountability*, che il trattamento è effettuato conformemente alle previsioni del GDPR; tra queste in particolare: i) la definizione del modello organizzativo, con attribuzione di ruoli e responsabilità, formalizzazione di nomine, definizione di processi, procedure e controlli tracciabili; ii) predisposizione ed erogazione di interventi formativi ed informativi in materia di protezione dei Dati Personali per i dipendenti e i soggetti che ricoprono ruoli specifici; iii) la creazione di strumenti operativi di supporto, quali il "*Vademecum in relazione ai compiti del Responsabile del Trattamento dei Dati Personali*", le "*Linee Guida sulle Persone Autorizzate al Trattamento dei Dati Personali*", la "*Policy sull'utilizzo degli strumenti IT*", nonché la "*Procedura per la gestione dei Data Breach*".

3.2.1 Informative e consensi

Il Gruppo Cerved si impegna a raccogliere i dati personali degli interessati che risultino necessari e pertinenti per le finalità perseguite nell'ambito delle rispettive attività statutarie, nel rispetto dei principi generali di liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione ed esattezza dei dati, limitazione della conservazione ed integrità e riservatezza dei dati (v. art. 5 GDPR) ed, a tal fine, adotta tutte le adeguate misure organizzative e tecniche volte a garantire la piene osservanza di tali principi.

Al momento della raccolta dei dati personali presso gli interessati o dell'acquisizione di tali dati da soggetti pubblici o privati diversi dall'interessato (nei limiti e termini consentiti dalle normative di riferimento), Cerved e le società del Gruppo Cerved, per quanto di rispettiva competenza, si impegnano a rendere agli interessati una preventiva ed idonea informativa contenente indicazioni chiare e specifiche sulle finalità e modalità del trattamento dei loro dati personali, sulla relativa base giuridica (consenso od altri presupposti di liceità, quali ad. es. l'esecuzione di un contratto, l'adempimento di obblighi legali od il perseguimento di legittimi interessi, come nel caso del perseguimento di finalità di informazione commerciale), sull'ambito di comunicazione a possibili destinatari dei dati, ivi inclusi soggetti stabiliti eventualmente in paese extra UE, sui tempi di conservazione dei dati, sui diritti spettanti agli interessati, nonché i riferimenti del Titolare del trattamento e i dati di contatto del DPO.

In particolare, al fine di adeguarsi alle previsioni del GDPR, il Gruppo Cerved:

- ha aggiornato i modelli di informativa ed eventuale richiesta di consenso in linea con i requisiti del GDPR (ad es. informativa per il Trattamento dei Dati Personali dei clienti, dei dipendenti, candidati, fornitori, visitatori, ecc.);
- raccoglie i diversi modelli in uso e la documentazione privacy ufficiale delle società del Gruppo Cerved in *repository* e li rende disponibili internamente nella sezione *intranet* dedicata e esternamente, per i documenti che hanno rilevanza tale, attraverso le apposite sezioni del sito internet www.cerved.com;
- definisce le modalità di aggiornamento/gestione dei modelli di informativa e consenso, nonché di loro consegna/comunicazione agli interessati e di raccolta, registrazione, conservazione degli eventuali consensi e revoche, identificando ruoli e responsabilità affidate ad organi/funzioni aziendali delle società del Gruppo Cerved.

3.2.2 Fornitori e soggetti esterni: contratti con i Responsabili del Trattamento

Il GDPR disciplina, sotto il profilo della protezione Dati Personali, l'eventualità che taluni Trattamenti siano eseguiti da soggetti esterni ("Responsabili del Trattamento") per conto del Titolare, precisando i ruoli e le responsabilità in capo rispettivamente al Titolare e al Responsabile del Trattamento.

Al riguardo, la fine di rispettare gli obblighi previsti dal GDPR sotto questo profilo, il Gruppo Cerved predispone:

- modelli di accordi o contratti (Data Processing Agreement - DPA), comprensivi di clausole specifiche (es. trasferimento dati extra EU, sub-responsabili, ecc.) e allegati, per disciplinare i rapporti con i Responsabili del Trattamento ed i relativi obblighi;
- specifiche istruzioni per la selezione e gestione dei fornitori, nonché le attività di sottoscrizione ed archiviazione dei relativi contratti;
- un'archiviazione dei modelli di contratto da adottare, oltre che dei contratti sottoscritti.

3.2.3 Registro dei trattamenti

Il registro dei Trattamenti ("**Registro**") ha un contenuto minimo previsto dal GDPR che varia a seconda che si tratti del Registro del Titolare o del Responsabile. Il Registro del Titolare contiene: (i) il nome e i dati di contatto del Titolare, del contitolare ove applicabile, del rappresentante del Titolare e del DPO; (ii) le finalità del Trattamento; (iii) una descrizione delle categorie di Interessati e dei Dati Personali; (iv) le categorie di destinatari a cui i Dati Personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; (v) 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; (vi) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di Dati Personali; (vii) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative. Il Registro del Responsabile contiene, oltre al sub (v) e al sub (vii): (i) il nome e i dati di contatto del Responsabile o dei Responsabili del Trattamento, di ogni Titolare per conto del quale agisce il Responsabile, del rappresentante del Titolare o del Responsabile e, ove applicabile, del DPO; (ii) le categorie dei Trattamenti effettuati per conto di ogni Titolare.

Al fine di assicurare il pieno rispetto delle disposizioni del GDPR in tema di registri delle attività di trattamento (art. 30), ogni società del Gruppo Cerved ha predisposto, tramite un apposito documento in formato elettronico, il Registro tenuto in qualità sia di Titolare che di Responsabile, contenente le informazioni obbligatorie sopra citate.

Tali Registri, a cui ha accesso anche il DPO per le sue attività di controllo, sono messi a disposizione delle strutture e consultabili tramite apposite cartelle condivise tra i Delegati Privacy e i Privacy Contact ai fini anche del relativo aggiornamento, in caso di avvio di nuovi Trattamenti, modifica o cessazione dei Trattamenti esistenti, che ogni struttura è tenuta ad effettuare o comunque a segnalare.

3.2.4 Tempi di conservazione dei Dati Personali

Nell'ambito delle informazioni da fornire all'Interessato, il Titolare è chiamato a verificare od individuare il periodo di conservazione dei Dati Personali Trattati, ovvero i criteri utilizzati per determinare tale periodo, decorso il quale i Dati Personali sono anonimizzati/cancellati.

Al fine di garantire il rispetto del principio di limitazione della conservazione sancito dal GDPR, il Gruppo Cerved pertanto definisce:

- linee guida sui criteri da seguire per individuare i tempi o termini di conservazione dei Dati Personali sulla base dei principi stabiliti dalla normativa privacy e dalle altre normative applicabili in relazione ai vari settori di ciascuna società del Gruppo Cerved;
- un processo operativo che disciplina le attività dei vari uffici di determinazione, validazione e controllo di nuovi termini di conservazione.

3.2.5 Data protection by design e data protection by default

Il Titolare, sin dalla progettazione del Trattamento ("*by design*"), mette in atto misure tecniche ed organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei Dati Personali, e ad integrare nel Trattamento le necessarie garanzie al fine di soddisfare i requisiti normativi e tutelare i diritti degli Interessati, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del Trattamento, come anche

dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal Trattamento.

Inoltre il Titolare garantisce che siano Trattati, per impostazione predefinita ("*by default*"), solo i Dati Personali necessari per ogni specifica finalità del Trattamento. Tale obbligo vale per la quantità dei Dati Personali raccolti, la portata del Trattamento, il periodo di conservazione e l'accessibilità.

Nel rispetto dei suddetti principi, tutte le strutture, direzioni, aree e *business unit* del Gruppo Cerved sono chiamate, in caso di ideazione e realizzazione di nuovi progetti, servizi, sistemi, ecc. che comportino attività di Trattamento dei Dati Personali a garantire i requisiti di *privacy by design* e *privacy by default*, seguendo la metodologia indicata a livello aziendale che hanno lo scopo di illustrare come le società del Gruppo Cerved abbiano adottato presidi interni (es.: policy/procedure, prassi consolidate e documentabili, misure di sicurezza) volti a far sì che i Trattamenti di Dati Personali svolti dalla medesima siano allineati a questi nuovi principi) e richiedendo apposite garanzie e funzionalità in tal senso anche ai fornitori, sviluppatori del *software*, ecc., in fase di relativa progettazione e a documentare le valutazioni effettuate. In particolare, laddove un nuovo progetto, servizio, sistema od attività riguardi od implichi un Trattamento di Dati Personali, la struttura che se ne occupa verifica le documentazioni anche tecniche, garanzie, funzionalità e misure adottate dal fornitore per assicurare la minimizzazione dei Dati Personali e dei possibili rischi che tale Trattamento può presentare per gli Interessati e coinvolge tempestivamente IT e il DPO per la valutazione della loro adeguatezza, fornendo loro tutti gli elementi e documenti a ciò necessari. Ove dalle verifiche svolte emerga che il Trattamento correlato al nuovo progetto, servizio od attività presenti un rischio elevato per i diritti degli Interessati la struttura procede ad avviare la procedura di DPIA di cui al successivo par. 3.2.8.. La struttura conserva comunque la complessiva documentazione raccolta anche dal fornitore in relazione alle verifiche ed attività svolte per il rispetto dei requisiti di *privacy by design/by default*.

3.2.6 Sicurezza dei Dati Personali

Il Titolare o il Responsabile del Trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del Trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, sono tenuti a mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono:

- la pseudonimizzazione e la cifratura dei Dati Personali;

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di Trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei Dati Personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento.

Per quanto riguarda i sistemi informatici e telematici, Cerved, tramite le competenti strutture IT, si impegna a definire le metodologie per l'effettuazione dell'analisi dei rischi per la sicurezza dei dati, nei termini sopra evidenziati, e per l'identificazione delle misure adeguate in relazione a tali rischi, verificando l'adeguatezza ed efficacia delle misure organizzative e tecniche adottate e da adottare al fine di garantire la conformità a quanto previsto dal GDPR e raccogliendo, conservando ed aggiornando la relativa documentazione.

Scopo dell'analisi dei rischi è individuare le minacce che possono originare rischi per i sistemi informatici, ed in generale per le informazioni trattate, e valutare se le misure di sicurezza poste in essere forniscono un adeguato livello di protezione. Lo svolgimento dell'analisi dei rischi non è un'attività meramente tecnica, svolta unicamente dal personale dell'area IT, ma è una valutazione che vede coinvolte tutte le aree delle organizzazioni del Gruppo Cerved per una analisi della situazione ambientale nei suoi aspetti più generali.

In nessun caso l'obiettivo di una politica di sicurezza può essere quello dell'eliminazione totale dei rischi, perché tale obiettivo sarebbe irraggiungibile: qualsiasi sistema di gestione delle informazioni, e, in particolare, quelli basati su strumenti tecnologici, è esposto a rischi che non possono essere totalmente eliminati. L'obiettivo deve essere quello di fornire un adeguato livello di protezione, valutato in base alla probabilità che un rischio si manifesti, alle conseguenze che ne deriverebbero, alla rilevanza delle informazioni trattate e all'insieme delle misure di protezione esistenti.

Cerved si impegna, dunque, a svolgere un'analisi critica dei rischi per la sicurezza dei dati e delle misure di protezione esistenti allo scopo di individuare le aree di vulnerabilità e, di predisporre o pianificare, le ulteriori misure di protezione che tali aree di vulnerabilità richiedono di implementare. La valutazione delle misure di sicurezza da implementare deriva quindi da un'attenta valutazione dell'efficacia delle misure di sicurezza poste in essere fino alla data dell'analisi, eseguita alla luce delle attuali condizioni tecnologiche ed organizzative.

L'analisi dei rischi viene, pertanto, condotta con periodicità prestabilita e, anche in base alla valutazione degli incidenti effettivamente accaduti, costituisce l'elemento portante dell'aggiornamento della politica generale della sicurezza.

L'analisi dei rischi fa riferimento ai comportamenti degli operatori, agli eventi dannosi che possono riguardare gli strumenti di elaborazione, agli eventi ambientali che riguardano in generale il contesto di Trattamento delle informazioni.

3.2.7 Notifica di Violazione dei Dati Personali (data breach)

Il Titolare del Trattamento è tenuto a notificare il data breach al Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. L'obbligo non ricorre qualora il Titolare sia in grado di dimostrare che è improbabile che la Violazione dei Dati Personali presenti un rischio per i diritti e le libertà delle persone fisiche. Il Titolare inoltre deve comunicare all'Interessato la Violazione dei Dati Personali senza indebito ritardo in caso di rischio elevato per i diritti e le libertà delle persone fisiche.

A tale scopo, il Gruppo Cerved ha adottato un'apposita procedura di gestione e notifica delle eventuali Violazioni di Dati Personali da notificare al Garante e, se del caso, comunicare agli Interessati, prevedendo anche la predisposizione di un registro delle violazioni, per documentare le valutazioni effettuate in proposito.

3.2.8 Data protection impact assessment (DPIA)

Il GDPR introduce l'ulteriore obbligo di provvedere ad una valutazione di impatto sulla protezione dei Dati - "*Data protection impact assessment*" – ("**DPIA**") per le attività di Trattamento avviate dal 25 maggio 2018 che presentino rischi elevati nei confronti degli Interessati, nelle ipotesi espressamente indicate dall'art. 35 e dall'elenco pubblicato dal Garante, nonché ricavabili dalle Linee Guida delle Autorità europee di protezione dei dati, nonché per le variazioni apportate, a partire da tale data, nei confronti di qualsiasi attività di Trattamento, qualora tali variazioni, anche per l'introduzione di nuove e più sofisticate tecnologie, abbiano rilevanti impatti sulla protezione dei Dati Personali, comportando un aumento dei rischi per i diritti degli Interessati.

Al fine di garantire l'osservanza degli obblighi appena evidenziati, prima di procedere ad un nuovo Trattamento di Dati Personali, la struttura del Gruppo Cerved che lo gestisce (c.d. *process owner*), consultandosi preventivamente con IT e con il DPO, è chiamata a verificare se tale Trattamento presenti "*un rischio elevato per i diritti e le libertà delle persone fisiche*" considerati la natura, l'oggetto, il contesto e le finalità del Trattamento, in particolare qualora sia previsto l'utilizzo di nuove tecnologie, e se rientri nei casi previsti dal GDPR e/o dal Garante, documentando le valutazioni effettuate. In caso affermativo, la *business unit* dovrà richiedere l'attivazione della

procedura di DPIA appositamente predisposta dal Gruppo Cerved, consultandosi con il DPO e le altre strutture interessate (IT), e, qualora la DPIA indichi che il Trattamento presenterebbe un rischio elevato nonostante le misure individuate per attenuare il rischio, proporre la consultazione preventiva del Garante.

3.2.9 Trasferimento dei Dati Personali verso Paesi terzi o organizzazioni internazionali

Il trasferimento di Dati Personali verso Paesi terzi (paesi al di fuori dell'Unione Europea o dello Spazio Economico Europeo) può avvenire in base al GDPR, solo se il Paese terzo garantisce un livello adeguato di protezione dei Dati Personali. La Commissione Europea ha il potere di stabilire tale adeguatezza attraverso una specifica decisione. Per quanto attiene ai paesi non inclusi in quelli considerati adeguati, in deroga al suddetto divieto, il trasferimento verso Paesi terzi può essere consentito anche sulla base di strumenti contrattuali che offrano garanzie adeguate.

In caso di trasferimento dei Dati Personali verso Paesi terzi, ogni funzione o struttura interessata di Cerved o delle società del Gruppo Cerved, prima di effettuarlo, si impegna a verificare:

- l'esistenza della decisione di adeguatezza dei Paesi terzi;
- per i Paesi Terzi ritenuti non adeguati dalla Commissione Europea, l'adozione di garanzie adeguate per i trasferimenti di Dati Personali in Paesi terzi, tra le quali:
  - il "*Privacy Shield*", cioè adesione all'accordo che regolamenta il trasferimento di Dati Personali tra Unione Europea e USA;
  - le "*Binding Corporate Rules*" (norme vincolanti di impresa), quale strumento contrattuale volto a consentire il trasferimento tra società facenti parti dello stesso gruppo d'impresa;
  - la sottoscrizione di "*Clausole Contrattuali Standard*", approvate dalla Commissione Europea.

  Le eventuali operazioni di trasferimento di dati in paese terzi extra UE, effettuate nel rispetto delle condizioni sopra indicate, sono oggetto di attento monitoraggio nell'ambito del Gruppo Cerved, in modo anche da permettere il costante aggiornamento ed allineamento degli altri adempimenti ad esse connessi (come, in particolare, i Registri dei trattamenti, le informative agli interessati, le misure di sicurezza).

3.2.10 Diritti dell'Interessato (artt. 15-22 GDPR)

All'Interessato è consentito l'esercizio dei seguenti diritti:

- diritto di accesso: diritto di ottenere dal Titolare la conferma che sia o meno in corso un Trattamento di Dati Personali che lo riguarda e in tal caso, di ottenere l'accesso ai Dati Personali e ad uno specifico set di informazioni (es. finalità del Trattamento, categorie di Dati Personali, etc…);

- diritto di rettifica: diritto di ottenere dal Titolare la rettifica dei Dati Personali inesatti che lo riguardano; tenuto conto delle finalità del Trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei Dati Personali incompleti, anche fornendo una dichiarazione integrativa;
- diritto alla cancellazione ("*diritto all'oblio*"): diritto di ottenere dal Titolare la cancellazione dei Dati Personali che lo riguardano senza ingiustificato ritardo e nell' obbligo del Titolare di cancellarli senza ingiustificato ritardo qualora ricorrano determinate condizioni;
- diritto di limitazione del Trattamento: diritto di ottenere dal Titolare una restrizione al Trattamento dei Dati Personali (ad es. la sola conservazione con esclusione di qualsiasi altro utilizzo) al ricorrere di determinate condizioni;
- diritto alla portabilità dei Dati Personali: qualora i Dati Personali siano Trattati con mezzi automatizzati, l'Interessato può richiedere al Titolare di (i) ricevere "*in un formato strutturato, di uso comune, leggibile da dispositivo automatico ed interoperabile*" un sottoinsieme di Dati Personali che lo riguardano e di conservarli in vista di un ulteriore utilizzo per scopi personali su supporto personale o su *cloud* privato; o (ii) trasferirli ad altro Titolare "*senza impedimenti*" e ove ciò sia tecnicamente fattibile;
- diritto di opposizione: consiste nel diritto dell'Interessato di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al Trattamento dei Dati Personali che lo riguardano effettuato per ragioni di interesse pubblico o per un legittimo interesse del Titolare, compresa la profilazione, nonché per finalità di *marketing* diretto;
- diritto di non essere sottoposto ad una decisione basata unicamente sul Trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla propria persona, a meno che ricorrano determinate condizioni in deroga.

Il Titolare fornisce riscontro agli Interessati a fronte di una delle suddette richieste senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (o al massimo entro ulteriori 2 mesi, in caso di richieste più complesse, ferma l'interlocutoria da dare sempre entro il primo mese).

Al fine di adeguarsi alle previsioni sopra riportate, il Gruppo Cerved:

- ha definito una procedura che disciplina la gestione e il riscontro delle richieste di esercizio dei diritti degli Interessati, identificando ruoli e responsabilità affidate ad organi/reparti aziendali del Gruppo Cerved, avente lo scopo di fornire indicazioni pratiche con riferimento alle richieste finalizzate all'esercizio dei diritti da parte degli Interessati ex artt. 15-22 GDPR

e al diritto di revoca del consenso ex art. 7.3 GDPR. La procedura identifica i canali di raccolta da cui queste richieste posso arrivare e ripercorre analiticamente le azioni da intraprendere per un puntuale riscontro dal punto di vista del Titolare, del Responsabile e contitolare del Trattamento;

- canali appositi per veicolare e raccogliere le richieste dagli Interessati;
- un registro in cui tracciare le richieste degli Interessati gestite dal Gruppo Cerved, ivi compresa la documentazione a supporto.

Definizioni (Glossario)

“Garante”	il Garante per la protezione dei Dati Personali.
“GDPR” o “Regolamento”	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).
“Codice privacy”	il d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, così come modificato dal d.lgs. 10 agosto 2018 n. 101, entrato in vigore il 19 settembre 2018 e recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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)”.
“Persona autorizzata”	qualsiasi persona fisica autorizzata ad accedere ai dati o a compiere operazioni di trattamento dal Titolare o dal Responsabile e che agisce sotto l’autorità di questi ultimi (es.: un dipendente o collaboratore incaricato del trattamento dei dati)
“Dato/i Personale/i”	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più

	elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
“Delegato privacy”	la persona fisica che, in virtù e nei limiti dei poteri di organizzazione, gestione e controllo conferiti dal Titolare, è delegata all’esercizio delle funzioni di direzione, coordinamento e controllo delle attività di trattamento dei dati personali e dei correlati adempimenti previsti dal GDPR.
“Privacy Contact”	la persona fisica che, individuata dal Delegato Privacy, coopera al fine di consentire il rispetto e l’attuazione delle procedure e le linee guida di cui si è dotata la società.
“Interessato”	la persona fisica identificata o identificabile a cui si riferiscono i Dati Personali.
“Responsabile del Trattamento”	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (es.: fornitore di servizi informatici)
“Responsabile Protezione Dati” o “DPO”	la figura (interna o esterna) nominata dal Titolare del trattamento quale Responsabile della Protezione dei Dati Personali ai sensi dell’art. 37 del GDPR.
“Titolare”	indica 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.
“Trattamento”	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica,

	l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
“Violazione dei Dati Personali”	la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

APPENDICE I - Principali adempimenti previsti dal GDPR

Principi applicabili al Trattamento di Dati Personali

Il GDPR (art.5) conferma sostanzialmente, oltre alle principali definizioni (oggettive di "*Dato Personale*" e "*Trattamento*" ed anche soggettive di "Titolare" o "Responsabile" del Trattamento) già previsti dalla previgente normativa, i principi generali applicabili al Trattamento dei Dati Personali, i quali prevedono che i Dati Personali siano trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato («*liceità, correttezza e trasparenza*»); raccolti per finalità determinate, esplicite e legittime, e successivamente Trattati in modo che non sia incompatibile con tali finalità («*limitazione della finalità*»); adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono Trattati («*minimizzazione dei Dati Personali*»); esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i Dati Personali inesatti rispetto alle finalità per le quali sono Trattati («*esattezza*»); conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono Trattati («*limitazione della conservazione*»); Trattati in maniera da garantire un'adeguata sicurezza dei Dati Personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da Trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («*integrità e riservatezza*»).

Informativa

In relazione alle informative sul Trattamento dei Dati Personali, gli articoli 13 e 14 del GDPR introducono alcuni elementi ulteriori rispetto a quelli previsti dalla precedente normativa, come l'esigenza di specificare la base giuridica del Trattamento, l'eventuale trasferimento di Dati Personali in Paesi terzi all'UE, il periodo di conservazione dei Dati Personali o i criteri seguiti per stabilire tale periodo, il diritto di presentare un reclamo all'autorità di controllo, oltre all'identità del Titolare, le finalità del Trattamento, i destinatari dei Dati Personali, i diritti degli Interessati, compreso il diritto alla portabilità dei Dati Personali, oppure se il Trattamento comporta processi decisionali automatizzati (anche la profilazione). Oltre ai contenuti, che in parte sono più ampi rispetto alla normativa previgente, il Titolare deve adottare misure appropriate per fornire all'Interessato le informazioni e le comunicazioni inerenti anche all'esercizio dei suoi diritti in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni possono essere fornite per iscritto o con altri mezzi, anche elettronici.

Presupposti di liceità del Trattamento (consenso e altri casi)

Dal punto di vista dei presupposti di liceità del Trattamento dei Dati Personali, il GDPR (artt. 6) conferma sostanzialmente quelli già previsti dalla previgente normativa, ossia il consenso (con sostanzialmente gli stessi requisiti: dichiarazione o azione positiva espressa in modo inequivoco od esplicito, libera, specifica, informata, da documentare adeguatamente) e una serie di casi di esclusione del medesimo consenso, come l'esecuzione del contratto o di misure precontrattuali richieste dall'Interessato, l'adempimento di obblighi legali, il perseguimento di legittimi interessi, in base ai quali il consenso rimane sostanzialmente da richiedere principalmente per le attività di *marketing* (es.: invio di comunicazioni commerciali con e-mail, fax, sms) e di eventuale profilazione dei clienti/utenti.

Per il Trattamento di Dati Particolari (ex sensibili, come salute, opinioni politiche, appartenenze sindacali, ecc.) e di dati relativi condanne penali e reati, il GDPR prevede casi di esclusione del consenso più ridotti (artt. 9 e 10), con l'eccezione dei Trattamenti dei Dati Personali dei dipendenti nell'ambito del rapporto di lavoro, per i quali, se correlati all'adempimento di obblighi normativi o di contrattazione collettiva, non occorre richiedere un consenso ai lavoratori. Inoltre, il GDPR (art. 9) lascia ai legislatori nazionali la possibilità di mantenere od introdurre ulteriori condizioni, comprese limitazioni, solo con riguardo al Trattamento di dati genetici, dati biometrici o dati relativi alla salute, le quali saranno declinate nelle misure di garanzia che il Garante è chiamato ad adottare ai sensi dell'art. 2-septies del Codice privacy. In relazione al Trattamento dei dati relativi a condanne penali e reati, l'art. 2-octies del Codice privacy prevede, altresì, che tale Trattamento è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, individuando un primo elenco di attività autorizzate a livello normativo (antiriciclaggio, difesa giudiziaria di diritti, informazioni commerciali, ecc.) e rinviando per il resto ad un regolamento da adottarsi con decreto del Ministero della Giustizia (sentito il Garante).

Diritti degli Interessati

Il GDPR rafforza il diritto alla cancellazione ("*diritto all'oblio*") e introduce il nuovo diritto di limitazione del Trattamento e il diritto alla portabilità (artt. 17, 18, 20 del GDPR), mentre conferma i diritti degli Interessati già previsti dalla normativa previgente, quali: il diritto di accesso, il diritto di rettifica e il diritto di opposizione.

Persone autorizzate al Trattamento

Il GDPR, pur non prevedendo espressamente la definizione di "*incaricati del Trattamento*" del Codice privacy (norma poi abrogata dal d.lgs. 101/18), fa riferimento alle "*persone autorizzate*

al trattamento dei dati personali sotto l'autorità diretta del titolare del trattamento o del responsabile del trattamento" e richiede sempre al Titolare o Responsabile del Trattamento di impartire a tale persone adeguate istruzioni sul medesimo Trattamento (artt. 29 e 32, ultimo par., GDPR), che devono essere documentate alla luce, come si dirà a breve, del nuovo principio di responsabilizzazione (*accountability*). Tale principio è stato declinato nell'ambito dell'art. 2-quaterdecies del Codice privacy, laddove, da un lato, si dispone che il Titolare o il Responsabile del Trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al Trattamento di Dati Personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità e, dall'altro, si prevede che possano essere individuate le modalità più opportune per autorizzare le persone al Trattamento dei Dati Personali.

APPENDICE II – Nuovi adempimenti previsti dal GDPR

Il GDPR introduce un cambiamento rilevante nella organizzazione e gestione degli adempimenti normativi in materia di privacy, rendendo necessario un sistema di "*governance*" dei Dati Personali, basato su una maggiore responsabilizzazione («*accountability*») del Titolare del Trattamento (art. 5), che deve garantire ed essere in grado di dimostrare la conformità («*compliance*») al GDPR. Tale nuova impostazione prevede per il Titolare l'obbligo di adottare misure tecniche ed organizzative la cui adeguatezza deve essere valutata sulla base delle specifiche caratteristiche dei Trattamenti di Dati Personali (natura, ambito di applicazione, contesto e finalità del Trattamento), nonché dei rischi per i diritti e le libertà delle persone fisiche (artt. 24). Sono connesse a questo cambiamento di impostazione organizzativa e gestionale anche tutte le principali novità introdotte dal GDPR.

Data Protection Officer (DPO) (Artt. 37-39)

La figura del DPO rappresenta una delle principali novità del GDPR e costituisce uno degli elementi-chiave della privacy compliance. La sua designazione è obbligatoria per tutti i soggetti ed organismi pubblici, mentre per i soggetti privati solo al ricorrere di determinati casi di Trattamento individuati dal medesimo GDPR (art. 37).

Il DPO è una figura che, in prima battuta, deve essere designato in funzione della sua conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati Personali, delle sue qualità professionali, della sua capacità di assolvere i propri compiti sopracitati, nonché della sua posizione di autonomia e indipendenza, riportando direttamente al vertice di ciascuna società del Gruppo Cerved.

I compiti principali del DPO sono quelli di informare e fornire consulenza sulla normativa applicabile in materia di protezione dei Dati Personali ai vertici aziendali, ai dipendenti della società del Gruppo Cerved che eseguono il Trattamento, nonché di sorvegliare l'osservanza del GDPR e delle politiche del Gruppo Cerved 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. Inoltre, il DPO coopera con il Garante e funge da punto di contatto per questioni connesse al Trattamento di Dati Personali, ed effettua, se del caso, consultazioni relativamente a qualsiasi altra questione, funge da punto di contatto per gli Interessati per tutte le questioni relative al Trattamento dei loro Dati Personali e all'esercizio dei loro diritti ed è chiamato a fornire pareri e svolgere le altre attività di competenza, in base alle procedure aziendali in vigore, nell'ambito dei processi di definizione

dei tempi di conservazione dei Dati Personali (*data retention policy*), di valutazione e notifica di un *data breach* e di svolgimento di una DPIA.

I dati di contatto del DPO, una volta individuato, devono essere pubblicati (in modo da essere conoscibili dagli interessati ed ai dipendenti) e comunicati al Garante.

Registro dei trattamenti (Art. 30)

Il GDPR introduce l'obbligo di tenere un Registro, sia per il Titolare del Trattamento, con riferimento alle attività di Trattamento svolte sotto la propria responsabilità, che per il Responsabile del Trattamento per le attività di Trattamento svolte per conto di un Titolare.

Data protection by design e by default (Art. 25)

Il GDPR prevede che, al momento dell'avvio di un nuovo Trattamento o della modifica di un Trattamento già in essere, il Titolare del Trattamento attui misure che soddisfino i principi di protezione dei Dati Personali (*data protection by design*) ed esorta il Titolare a mettere in atto misure tecniche e organizzative adeguate per garantire che siano Trattati, per impostazione predefinita, solo i Dati Personali necessari per ogni specifica finalità del Trattamento (*data protection by default*).

Data Protection Impact Assessment - DPIA (Art. 35)

Il GDPR prevede che, qualora un Trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare effettui, prima di procedere al Trattamento, una valutazione d'impatto sulla protezione dei Dati Personali.

Notifica di un data breach (Artt. 33 e 34)

Il GDPR introduce l'obbligo di notificare al Garante, senza ingiustificato ritardo (e, ove possibile, entro 72 ore), eventuali violazioni dei Dati Personali, nonché di comunicarle anche agli Interessati senza ingiustificato ritardo laddove vi sia un rischio elevato per i diritti e le libertà delle persone fisiche.

Responsabile del Trattamento (Artt. 28 e 82)

Il GDPR individua specifici obblighi e responsabilità in capo anche ai Responsabili del Trattamento. Il Responsabile, inoltre, può ricorrere ad un altro Responsabile ("*sub-responsabile*") previo autorizzazione del Titolare, imponendo al sub-responsabile, tramite contratto o altro idoneo atto giuridico, le stesse obbligazioni assunte dal medesimo Responsabile nei confronti del Titolare.

Sicurezza del Trattamento (Art. 32)

Rispetto alla normativa previgente, il GDPR conferma la rilevanza degli obblighi in tema di sicurezza dei dati, ma non prevede più misure "*minime*" di sicurezza, poiché prescrive in capo

al Titolare ed al Responsabile l'obbligo di adottare misure tecniche ed organizzative adeguate al rischio.

Certificazione dei Trattamenti (Artt. 42 e 43)

Il GDPR introduce la facoltà di aderire ad una certificazione privacy (o sigilli e marchi di protezione dei dati), che possono assumere rilevanza ai fini dell'attestazione della conformità al GDPR.

Sanzioni amministrative pecuniarie (Art. 83)

Il GDPR non prevede sanzioni penali (lasciando ai legislatori nazionali la possibilità di mantenerle od introdurne di nuove), ma aumenta in modo rilevante l'importo massimo delle sanzioni, prevedendo la possibilità per il Garante di irrogare sanzioni amministrative fino all'importo di Euro 10.000.000 o, per le imprese, se superiore, al 2% del fatturato globale annuo, ovvero fino all'importo di Euro 20.000.000 o, per le imprese, se superiore, al 4% del fatturato globale annuo, a seconda delle disposizioni violate.

A seguito della revisione del Codice privacy, sono state mantenute e integrate alcune sanzioni penali volte a colpire le condotte illecite più gravi (commesse con dolo specifico, ossia al fine di trarre profitto od arrecare danno all'interessato) relative, in particolare, al Trattamento illecito dei Dati Personali riguardanti Categorie Particolari di Dati Personali o relativi a condanne penali e reati (nonché i dati di traffico telefonico/telematico, di localizzazione, le comunicazioni indesiderate. V. art. 167 Codice privacy); comunicazione o diffusione illecita di Dati Personali oggetto di Trattamento su larga scala (art. 167-bis); acquisizione fraudolenta di Dati Personali trattati su larga scala (art. 167-ter); falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o nell'esercizio dei poteri del Garante (art. 168); inosservanza dei provvedimenti del Garante (art. 170). Restano infine ferme le sanzioni penali previste per le violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (artt. 4, 8 e 38 della legge 300/1970 – Statuto dei lavoratori).