Regolamento Aziendale di Accountability

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI RELATIVO AL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (UE) 2016/679

DIMITTO®
CERTIFICATION SERVICES

www.dimitto.com

Regolamento aziendale di Accountability relativa al GDPR (UE) 2016/679

PARTE PRIMA: INTRODUZIONE

PARTE SECONDA: DISPOSIZIONI GENERALI

PARTE TERZA: DIRITTI DELL'INTERESSATO

PARTE QUARTA: TITOLARE E RESPONSABILE DEL TRATTAMENTO

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI

MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

PARTE SESTA: ATTUAZIONE IN AMBITO AZIENDALE DEGLI ADEMPIMENTI EUROPEI

ALLEGATI AL REGOLAMENTO AZIENDALE DI ACCOUNTABILITY

PARTE PRIMA

1: NORMATIVA

Il presente Regolamento aziendale di accountability in materia di protezione dei dati personali ("privacy") è uno strumento di applicazione del vigente Decreto Legislativo 30 giugno 2003, n. 196 ("Codice sulla privacy") e, in particolare, del nuovo Regolamento Generale sulla protezione dei dati personali (UE) 2016/679, e del Decreto Legislativo 18 maggio 2018 nr. 51 (attuazione della direttiva (UE) 2016/680 del 27 aprile 2016) nell'ambito dell'organizzazione dell'Azienda il quale per sua natura sostituisce ed annulla le disposizioni non conformi del Codice sulla privacy fino alla promulgazione del nuovo codice. In questo documento il Regolamento citato potrà essere in modo alternativo chiamato "GDPR", "RGPD", o "Regolamento Europeo sulla privacy" oppure semplicemente "Regolamento" o "Regolamento Europeo" o "Regolamento UE" intendendosi sempre 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 tali dati e che abroga la direttiva 95/46/CE

A far data dal 25 maggio 2018 trova diretta applicazione, sul territorio nazionale il Regolamento Europeo sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016.

Il Regolamento disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.

La sua entrata in vigore è stabilita il 24 maggio 2016: entro due anni a partire da tale data, e quindi entro la data del 25 maggio 2018, tutti gli Stati membri dell'Unione europea debbono uniformarsi alle nuove regole comunitarie, evitando così di incorrere nelle pesanti sanzioni (sia economiche sia di natura penale disciplinate in ogni singola nazione) previste dal nuovo Regolamento Generale sulla protezione dei dati personali (UE) 2016/679.

La data del 25 maggio 2018 è inderogabile, in quanto le prescrizioni stabilite dal Regolamento Generale sulla protezione dei dati personali (UE) 2016/679 trovano diretta ed immediata applicazione, indipendentemente dalla preesistenza di differenti norme nazionali in materia che, quindi, sono automaticamente superate dai precetti del Regolamento Europeo. Il fine del Regolamento Generale sulla protezione dei dati personali (UE) 2016/679 è infatti quello di armonizzare il trattamento dei dati all'interno dell'Unione Europea e dello Spazio Economico Europeo.

Ciò comporta che le disposizioni legislative di cui al Codice della privacy (D.lgs. 196/2003 e segg.), così come le norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali, siano superate, a far data dal 25 maggio 2018, da quelle del Regolamento UE, nella misura in cui le norme nazionali siano contrastanti o incompatibili con quelle europee.

Si segnala che, alla data di redazione della presente edizione del Regolamento aziendale di accountability, il Legislatore italiano si è attivato pubblicando in Gazzetta Ufficiale 06.11.2017 n. 259 la Legge Delega 25 ottobre 2017 n. 163 che, all'articolo 13, delega il Governo ad adeguare la legge italiana sulla privacy (D.lgs. 196/2003) alle nuove disposizioni europee e il Decreto Legislativo 18 maggio 2018 nr. 51 (attuazione della direttiva (UE) 2016/680 del 27 aprile 2016). Si indica inoltre che il Legislatore italiano ha novellato l'attuale D.lgs 196 del 30 giugno 2003 attraverso il D.lgs 101 del 10 agosto 2018 in ottemperanza al regolamento GDPR (UE) 2016/679.

Il presente Regolamento aziendale di accountability è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

2: ORGANIZZAZIONE

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-consumatore-utente che si rivolge alla impresa, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla privacy costituisce, anche secondo il Legislatore europeo, un vero e proprio diritto inviolabile dell'essere umano, che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità del singolo individuo. (Art. 1 GDPR (UE) 2016/679).

Per questi motivi, la "cultura della privacy" necessita di divenire un vero e proprio elemento cardine dell'organizzazione di questa impresa, che deve impegnarsi perché la cultura di cui si tratta possa crescere e rafforzarsi, principalmente fra gli operatori dell'impresa e i collaboratori, in quanto solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di carattere tecnico ed organizzativo, nel trattamento dei dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con i clienti, i fornitori, i consumatori e gli utenti in generale dei servizi che vengono da noi erogati

3: METODOLOGIA

Vengono allegati a questo Regolamento aziendale di accountability una serie di documenti necessari a dare compiuta attuazione, sia verso l'interno che verso l'esterno, ai dettami della nuova "privacy europea", al fine di ottemperare agli obblighi previsti dal Regolamento generale sulla protezione dei dati (UE) 2016/679.

Tra questi documenti, assieme a questa relazione di accountability, responsabilizzazione e rendicontazione attività per l'adeguatezza al GDPR all'evoluzione della materia (Capo IV Art 24.) vi sono, a titolo esemplificativo:

1. Elaborazione Organigramma Privacy, verifica eventuali contitolarità (Art. 26).
2. Stesura del Registro dei Trattamenti del Titolare e del Responsabile (art. 30 paragrafo 1 e paragrafo 2).
3. Elaborazione informative interessati (Art. 13, Art. 14) quali: Clienti/Utenti, Dipendenti, Collaboratori, Responsabili esterni.
4. Lettere di nomina da parte del Titolare del trattamento e suo procuratore dei delegati, incaricati e responsabili esterni (Art. 28), Data Protection Officer, se necessario (Art. 37).
5. Disciplinare interno incaricati e linee guida informatiche di base per la gestione degli accessi con password ai computer.
6. Verifica trasferimento dati all'esterno, incluse policy di backup incloud (adeguatezza, privacy shield…) (Capo V).
7. Verifica web, social e suggerimento di applicazione linee guida cookie policy oltre alle informative da utilizzarsi online (Capo III).
8. Predisposizione piano di formazione del personale sul GDPR: fornitura documenti ufficiali da parte del Garante Italiano in versione pdf, copia del Regolamento Generale sulla protezione dei dati.
9. Piano di verifica e di aggiornamento.

Questo Regolamento aziendale di accountability costituisce strumento propedeutico all'applicazione del regolamento medesimo, che ne è conseguenza dal punto di vista logico e temporale e che ne costituisce, appunto, il risultato attuativo in termini di azioni aziendali nel frattempo poste in essere per ottemperare agli obblighi europei.

E' doveroso infatti rimarcare, sin da ora, che il principio cardine introdotto dal nuovo Regolamento UE è quello della "responsabilizzazione" (accountability nell'accezione inglese) che pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della "conformità" o compliance nell'accezione inglese); vi è quindi l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato al Titolare del trattamento il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento Europeo.

Questa impresa, nella figura del suo legale rappresenta protempore, ha fatto proprio l'approccio del Legislatore europeo relativo all'accountability ed alla compliance, adottando appunto le misure ritenute adeguate ed in evoluzioni per ottemperare alle normative in vigore.

PARTE SECONDA: DISPOSIZIONI GENERALI

4: OGGETTO DEL REGOLAMENTO AZIENDALE

Il presente Regolamento aziendale di accountability disciplina, all'interno dell'impresa, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali (Decreto Legislativo del 30/06/2003 n. 196) ed in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE n. 679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

5: FINALITÀ' DEL REGOLAMENTO

L'impresa garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato. La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea.).

6: SENSIBILIZZAZIONE e FORMAZIONE

Il Titolare del Trattamento sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto ai clienti e consumatori. A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale aziendale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'impresa.

Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento europeo, e di conseguenza dal presente nuovo Regolamento aziendale, ad ogni dipendente (oltre che ad ogni collaboratore, consulente o tirocinante) viene rilasciata una specifica lettera di incarico con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali "incaricati ed autorizzati al trattamento dei dati" ai sensi del D.lgs. 196/2003 e del Regolamento UE 2016/679". Il personale indicato inoltre verrà formato con cadenza annuale, ove ve ne sia la necessità in base a modifiche sopravvenute delle norme, leggi, provvedimenti e regolamenti nonché tecnologie innovative informatiche e procedure non informatiche attraverso gli strumenti formativi ritenuti idonei dal Titolare del trattamento

7: DEFINIZIONI

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo Regolamento aziendale si intende per (tra parentesi i *considerando* o gli *articoli* relativi del GDPR (UE) 2016/679):

1) «dato personale»: 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; (C26, C27, C30);

2) «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;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (C67)

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (C24, C30, C71-C72)

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conserva- te separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (C26, C28-C29)

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; (C15)

7) «titolare del trattamento»: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (C74)

8) «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;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (C31)

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; (C32, C33)

12) «violazione dei dati personali»: ´*data breach*, in inglese) 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; (C85)

13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acqui- site di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; (C34)

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (C51)

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (C35)

16) «stabilimento principale»: (C36, C37)

- a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
- b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del Regolamento europeo; (C80)

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate; (C37, C48)

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati persona- li applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune; (C37, C110)

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: (C124)

- a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autoritàà di controllo;

- b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

- c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al pre- sente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

8: PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 5 del Regolamento Europeo n. 2016/679, i dati personali trattati dall'impresa sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»)

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali («limitazione della finalità»)

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalitàà per le quali sono trattati («minimizzazione dei dati»)

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»)

e) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»)

f) 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»).

9: TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (*ex DATI SENSIBILI/GIUDIZIARI*)

Si dà atto che questa impresa può venire a conoscenza ai fini dell'assolvimento della prestazione e solo collegando tale conoscenza alla prestazione stessa, escludendo qualsiasi atra tipologia di trattamento, archiviazione, comunicazione o diffusione, di dati particolari forniti in modo esplicito da parte dell'interessato.

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Detta disposizione relativa all'art 9 del Regolamento europeo non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato articolo n. 9, meritevoli di interesse relativamente alla attività di questa impresa in ambito specificamente relativo al comma 2, ai paragrafi a), b), c), e), h) e comma 3. Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati sensibili, biometrici e genetici e in particolare con le "Autorizzazioni generali", dall'Autorità Garante per la protezione di dati personali.

10: TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679, "il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica."

Si dà atto che il contenuto dell'anzidetto articolo n. 10 del Regolamento UE è rispondente alle vigenti disposizioni di cui al Codice della privacy, anche con riferimento al contenuto della lettera "e" rubricata "dati giudiziari" dell'articolo n. 4 del Codice della privacy D.lgs. 196/2003 e segg. Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati giudiziari e in particolare con le "Autorizzazioni generali", dall'Autorità Garante per la protezione di dati personali.

11: COMUNICAZIONE DI DATI VERSO L'ESTERNO

La comunicazione di dati sensibili e giudiziari da parte del titolare è ammessa solo quando quando è prevista da una norma di legge o regolamento e comunque quando è ritenuta necessaria per lo svolgimento di funzioni prestazioni che hanno ricevuto esplicito consenso da parte dell'interessato, anche a seguito di un bilanciamento degli interessi in gioco.

PARTE TERZA: DIRITTI DELL'INTERESSATO

12: INFORMATIVA SUL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 13 del Regolamento Europeo nr. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, ovvero dell'articolo 14 del Regolamento Europeo nr. 2016/679 (informazioni fornite qualora i dati personali non siano stati ottenuti presso l'interessato) il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante

b) i dati di contatto del Responsabile della protezione dei dati (D.P.O.) ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) dove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

f) l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.

13: CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

Il Regolamento UE conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceitàà del trattamento sono indicati all'art. 6 del Regolamento Europeo e coincidono, in linea di massima, con quelli previsti attualmente dal vigente Codice della privacy (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

In particolare:

a) per i dati particolari "sensibili" il consenso deve essere "esplicito". Lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione, articolo 22). Detta disposizione relativa all'art 9 del Regolamento europeo non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato articolo n. 9, meritevoli di interesse relativamente alla attività di questa impresa in ambito specificamente relativo al comma 2, ai paragrafi a), b), c), e), h), i) e comma 3.

b) non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati particolari *ex sensibili)* è ritenuto da questa impresa necessario e documentabile; inoltre, il Titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento

c) Il consenso dei minori è valido a partire dai 16 anni: prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci (articolo n. 8 del Regolamento Europeo)

d) deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare "caselle pre-confermate" su un modulo); deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile"

e) Interesse vitale di un terzo: si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione (C46).

Interesse legittimo prevalente di un titolare o di un terzo:

a) Il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso Titolare; si tratta di una delle principali espressioni del principio di Accountability, "responsabilizzazione" introdotto;

b) l'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità;

c) il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

14: DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) 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;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) 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;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonchéé l'importanza e le conseguenze previste di tale trattamento per l'interessato.

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'articolo 46 relative al trasferimento.

Il Titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

L'interessato ha diritto di ottenere una copia di cui al capoverso precedente non deve ledere i diritti e le libertà altrui.

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'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.

In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni possono essere fornite in un formato elettronico di uso comune.

Per quanto riguarda le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed organizzativo, il diritto di accesso, si fa rinvio alle vigenti disposizioni normative e regolamentari emanate, negli anni, dal Legislatore nonché dal Garante per la privacy, con particolare riferimento all'ambito dei dati particolari

15: DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

16: DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 2016/679, in capo all'interessato è riconosciuto il diritto "all'oblio", che 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" (Art 17, paragrafo 2 del Regolamento UE).

17: DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche 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 diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

18: DIRITTO ALLA PORTABILITA' DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche 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, sono portabili solo i dati trattati con il consenso dell'interessato o 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, per esempio), e solo i dati che siano stati "forniti" dall'interessato al Titolare (C 68).

Inoltre, il Titolare del trattamento deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

19: DIRITTO DI OPPOSIZIONE

Come stabilito dall'articolo n. 21 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni. Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

20: PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

Come stabilito dall'articolo n. 22 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di non essere sottoposto a 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 sua persona.

Tale principio non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;

c) si basi sul consenso esplicito dell'interessato.

PARTE QUARTA

TITOLARE E RESPONSABILE DEL TRATTAMENTO

21: TITOLARE DEL TRATTAMENTO

Il **"Titolare" del trattamento** dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti del vigente Codice della privacy, è DIMITTO Italia Srl, rappresentata nella persona di ZACCAGNINO MARIALUISA in qualità di Amministratore Unico dell'impresa stessa, con sede Legale in Milano (MI), Via Freguglia 2, e sede Operativa in Tito (PZ) Contrada Santa Loja Snc.

Il Titolare provvede:

a) a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;

b) a nominare con atto di nomina i Responsabili del trattamento dei dati personali, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy e all'articolo 12 del Regolamento UE, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;

c) a nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE laddove gli estremi dell'arti 37 che ne prevede la nomina anche ai sensi della circolare dell'autorità italiana nr. 8036793 del 26/03/2018, se previsto;

d) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;

e) a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento aziendale di accountability.

Questa impresa nella persona del suo legale rappresentante, ha fatto proprio l'approccio del Legislatore europeo relativo all'accountability sin dalla adozione del presente Regolamento aziendale di accountability relativa alle azioni aziendali utili ad ottemperare alle previsioni legislative di matrice europea.

22: CONTITOLARI DEL TRATTAMENTO

Come stabilito dall'articolo n. 26 del Regolamento Europeo n. 2016/679, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

23: RESPONSABILE INTERNO (DELEGATO E INCARICATO) DEL TRATTAMENTO DEI DATI

Il D.lgs. 196/2003, intende per Responsabile del trattamento dei dati, "la persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione ed Organismo preposti dal Titolare al trattamento di dati personali".

Il Regolamento Europeo (art. 28) disciplina i compiti del Responsabile esterno senza contemplare espressamente la figura ed i compiti del Responsabile interno.

Nella nostra realtà d'impresa saranno considerati delegati o incaricati del trattamento coloro i quali, per delega da parte del Titolare del trattamento, saranno autorizzati da parte del Titolare del trattamento, al trattamento dei dati e tenuti allo stesso trattamento ai soli fini dei compiti previsti o del trattamento previsto a trattare i dati personali degli interessati.

Nel caso si necessiti di una struttura più complessa in ambito ai processi, comparti e organigramma manageriale, sarà compiti di questa impresa rivedere e aggiornare tali deleghe ed identificare persone chiave "responsabili interni del trattamento" con funzioni dirigenziali apicali nei confronti degli incaricati. Teli necessità potranno essere rilevate in sede di audit e valutazione annuale o quando le necessità di impresa lo richiedano.

Il Titolare del trattamento dei dati deve informare ciascun delegato ed incaricato al trattamento dei dati, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti.

I delegati ed incaricati al trattamento rispondono al Titolare del trattamento di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

Ogni delegato o incaricato del trattamento deve:

a) trattare i dati personali, anche sensibili, osservando le disposizioni del presente Regolamento aziendale di accountability nonché le specifiche istruzioni impartite dal Titolare del trattamento;

b) garantire che, nello svolgimento delle proprie mansioni il trattamento dei dati personali garantisca un adeguato livello di riservatezza;

c) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi e mansioni affidate il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché dell'eventuale segreto professionale, fermo restando quanto previsto dalla normativa vigente;

d) tenendo conto della natura del trattamento, assistere, per quanto possibile, il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;

e) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel presente Regolamento;

f) contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

24: RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

Nell'ambito dell'attività d'impresa di questa realtà sono inoltre individuati quali Responsabili esterni del trattamento dei dati personali, tutti i soggetti esterni che, per svolgere la propria attività sulla base di un rapporto contrattuale con la stessa società committente, trattino dati di cui è titolare la società committente medesima e qualora siano in possesso dei requisiti previsti dall'articolo 29, primo comma, del Codice della privacy (esperienza, capacità ed affidabilità).

In ottemperanza all'articolo 29 del D.lgs. 196/2003 e, in particolare, ai sensi del nuovo articolo 28 del Regolamento Europeo 2016/679, i Responsabili esterni hanno l'obbligo di:

a) trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;

b) trattare i dati personali, anche eventualmente di natura particolare, degli interessati esclusivamente per le finalità previste dal contratto con la società committente e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;

c) rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;

d) adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento Europeo nr. 2016/679;

e) nominare, al loro interno, i soggetti autorizzati / incaricati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;

f) attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;

g) specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure adeguate di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.

h) assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo (sicurezza del

trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

i) su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;

j) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento Europeo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Nel caso di mancato rispetto delle predette disposizioni e in caso di mancata nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso il Titolare del trattamento, il Responsabile esterno del trattamento.

La designazione del Responsabile esterno viene effettuata mediante lettera di nomina sottoscritta da parte del Titolare del trattamento ed inviato al Responsabile esterno del trattamento in modo certo e documentabile, con previsione di firma per accettazione dell'incarico da parte del Responsabile esterno: il documento deve essere richiamato dagli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente all'Azienda.

L'accettazione della nomina a responsabile del trattamento e l'impegno a rispettare le disposizioni della nomina stessa è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

25: INCARICATO (AUTORIZZATO) INTERNO ED ESTERNO DE TRATTAMENTO DEI DATI

Il Regolamento Europeo non fornisce rilievo autonomo alla figura dell'incaricato al trattamento dei dati, seppure si soffermi sul fatto che chi tratta dati, ricevendo istruzioni e formazione da parte del Titolare del trattamento debba da questi essere "autorizzato" al trattamento (articoli 4 e 10 del Regolamento Europeo): cosicché si rinvengono nell'autorizzato al trattamento significative sovrapposizioni con l'incaricato del trattamento dei dati previsto dal D.lgs. 196/2003, a cui si rinvia.

Come già stabilito dal presente Regolamento aziendale di accountability, al momento dell'attivazione del contratto di lavoro o di collaborazione è fornita, a cura dell'impresa, ad ogni dipendente (oltre che ad ogni collaboratore, consulente o tirocinante) una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i summenzionati soggetti non dipendenti), con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali "incaricati ed autorizzati al trattamento dei dati" ai sensi del D.lgs. 196/2003 e del Regolamento UE 2016/679.

Il Regolamento Aziendale di Accountability in materia di Protezione dei Dati Personali relativo al GDPR (UE) 2016/679 è consultabile in azienda, e contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento aziendale di accountability e delle modalità di consultazione del medesimo.

Analoghe considerazioni valgono per la figura dell'incaricato / autorizzato esterno: tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito di questa impresa, pur non essendo dipendenti e neppure titolari di incarichi conferiti dalla medesima Azienda (quali consulenze, collaborazioni o tirocini), devono essere designati da parte del Responsabile esterno tramite una lettera (o una nota) di nomina come incaricati esterni.

Ci si riferisce, a titolo esemplificativo, al personale tirocinante o al personale volontario che opera temporaneamente all'interno dell'Azienda in virtù di un accordo o di una convenzione con un Ente esterno pubblico o privato (es. Associazione di volontariato o Ente universitario, Istituto per inserimento al lavoro) per lo svolgimento, appunto, ad esempio di tirocini formativi. Il personale di cui si parla è soggetto agli stessi obblighi cui sono sottoposti tutti gli incaricati "interni", in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.

Nel caso di Incaricati esterni, l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attivitàà.

26: RESPONSABILE AZIENDALE DELLA PROTEZIONE DEI DATI

Il Regolamento Europeo impone la nomina del Data Protection Officer (in italiano: Responsabile della protezione dei dati o 'RDP'), nei termini di cui all'articolo 37, 38 e 39 del Regolamento stesso. La nomina del RDP è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come attività principali i dati sensibili su larga scala, come ospedali, imprese assicuratrici e istituti di credito oltre alle realtà indicate dall'autorità Garante Italiana con documento nr. 8036793. Del 26/03/2018.

Chi svolge la funzione di RPD, quindi, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, inoltre, essere in conflitto di interessi in quanto il Regolamento UE vieta di nominare RDP anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi.

Ai sensi dell'articolo 39 del Regolamento UE, i suoi compiti sono:

a. sorvegliare l'osservanza del Regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;
b. fornire consulenza e pareri al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
c. collaborare con il titolare, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
d. informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
e. cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
f. supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

Ai sensi dell'articolo 37 del Regolamento UE, Egli deve:

a) possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;

b) adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;

c) operare alle dipendenze del titolare oppure sulla base di un contratto di servizio (RPD esterno);

d) disporre di risorse umane e finanziarie, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Questa impresa per le funzioni, le attività, la compagine societaria e la tipologia di dati trattati anche a seguito di autorizzazione ministeriale ritiene al momento della stesura di questo aggiornamento non obbligatoria la contrattualizzazione del Responsabile della Protezione dei dati (RPD, DPO, Data Protection Officer).

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI

MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

27: PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE (privacy by design) E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA (privacy by default)

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese *privacy by design* e *privacy by default*, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. (C75-C78)

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento Europeo nr. 2016/679 e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

Per le modalità organizzative con le quali questa impresa ha stabilito di ottemperare all'adempimento sin qui descritto, ci riferiamo agli allegati a questo Regolamento aziendale di accountability con le azioni di carattere organizzativo, gestionale e documentale.

28: REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento. L'autorità Garante italiana e gli organi preposti alla vigilanza sull'ottemperanza del Regolamento Europeo e normativa in materia di privacy, hanno più volte sottolineato che, nonostante esso sia obbligatorio con le esclusioni del paragrafo 5 art. 30 GDPR (UE) 2016/679, il registro dei trattamenti è alla base delle attività svolte e strumento di verifica, pianificazione, gestione e controllo. Con il comunicato del Garante Privacy del giorno 8 ottobre 2018 il Garante per la protezione dei dati personali ha indicato categorie e procedure suggerite per redigere il registro oltre che indicare un modello, qui aggiunto e utilizzato, per le PMI.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio dove necessaria.

La tenuta del Registro del Trattamento in forma cartacea oppure elettronica dei trattamenti, con le indicazioni principali previste dall'art. 30 comma costituisce parte integrante del Regolamento aziendale di accountability e viene custodito dall'azienda e mostrato in caso di necessità.

In esso sono contenute le seguenti informazioni:

A. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

B. le finalità del trattamento; una descrizione delle categorie di interessati e delle categorie di dati personali;

C. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

D. 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;

E. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

F. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

29: PROTEZIONE E SICUREZZA DEI DATI PERSONALI

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, secondo il Regolamento Europeo 2016/679 non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al Titolare del trattamento e al Responsabile esterno in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilitàà di utilizzare l'adesione a specifici codici di condotta quando adottati o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza intraprese, oltre a prevedere eventuali azione minime suggerite per talune imprese e taluni dati come indicato nel D.lgs. 101 del 10 agosto 2018.

30: NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO (DATA BREACH)

A partire dal 25 maggio 2018, tutti i titolari, e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi, dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del Regolamento UE); questa procedura va sotto il nome di "Data Breach".

Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare del trattamento.

Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del Regolamento Europeo. Su questo e su tutta la disciplina in materia, il Comitato europeo della protezione dati (si

veda art. 70, paragrafo 1, lettere g e h) è chiamato a formulare linee-guida specifiche, alle quali sta già lavorando il Gruppo WP29.

Il Titolare del trattamento, sentito il Data Protection Officer aziendale laddove presente, adotta le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Il Modello per la notifica dei data breach è fornito sul sito dell'Autorità italiana

Il predetto modello è allegato al presente Regolamento aziendale di accountability

31: VALUTAZIONE DI IMPATTO (PIA - PRIVACY IMPACT ASSESMENT) SULLA PROTEZIONE DEI DATI

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse al secondo criterio individuato nel Regolamento UE rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento.

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (C75 C77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All'esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

32: TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Si fa rinvio ai principi dettati dal Regolamento Europeo agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali. Le eventuali trasmissioni di dati all'esterno quando comunicate all'interessato avverranno esclusivamente sulla base di valutazioni caso per caso di paesi ritenuti adeguati, con clausole contrattuali, BCR o "scudo della privacy" (Privacy Shield USA-UE).

33: VIDEOSORVEGLIANZA

Al momento della edizione di questo documento l'impresa ha presentato l'istanza di autorizzazione per l'installazione di impianti di videosorveglianza con *nr protocollo 39553 del 12 novembre 2015* al Ministero del Lavoro e delle Politiche Sociali Direzione Territoriale del Lavoro della Basilicata e non ha ricevuto autorizzazione specifica in quanto non dovuta per la mancanza del presupposto ex art 4 Legge 300/70 sulla registrazione durante orario di lavoro. Nel momento dell'attuazione della videosorveglianza per la tutela del patrimonio in orari differenti da quello indicato nel protocollo di cui sopra, saranno adottate le specifiche attività normative del caso secondo le leggi vigenti in materia e il Regolamento Europeo oltre all'ottemperanza di ogni leggi in ambito dello Statuo del Lavoratori Legge 20 maggio 1970 nr. 300.

34: UTILIZZO DEI MEZZI INFORMATICI E TELEMATICI

In merito all'utilizzo dei mezzi informatici e telematici si rinvia al apposito disciplinare.

PARTE SESTA

ATTUAZIONE

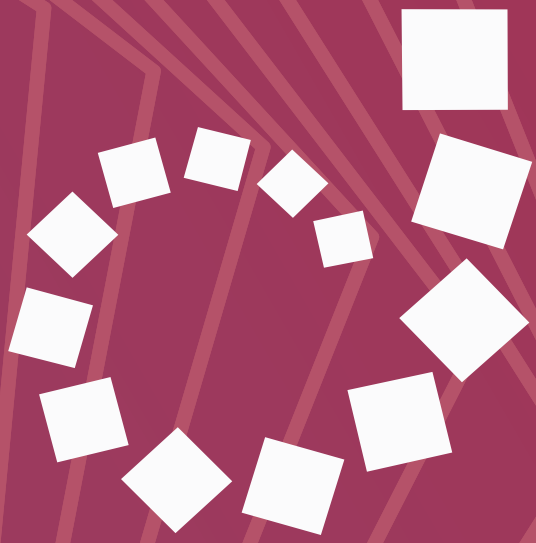
35: ADEMPIMENTI

In merito alla valutazione (Audit) e alle eventuali osservazioni e correzioni in merito all'applicazione del Regolamento generale sulla protezione dei dati (UE) 2016/679, questa impresa ha individuato gli ambiti di attività aziendale per ottemperare al Regolamento Europeo stesso con le prime iniziali attività previste che si configurano nelle attività strategiche e organizzative, documentali, tecnologiche ed informatiche oltre che comunicative e formative ed in particolare nello sviluppo delle attività relativa al processo di accountability previsto dal Regolamento Europeo ad alla base di questo Regolamento aziendale.

36: ENTRATA IN VIGORE

Il presente Regolamento aziendale di accountability entra in vigore al momento della sua adozione.

Questo Regolamento aziendale di accountability potrà essere aggiornato con altro documento, a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, sia nazionale, europeo o regionale, in materia di protezione dei dati personali.



Regolamento di Accountability GDPR (UE) 2016/679 Ed.B 17/01/2020