Deliberazione della Giunta Regionale 9 agosto 2019, n. 1-192

Ulteriori adempimenti in attuazione del Regolamento (UE) 2016/679 (GDPR). Approvazione "Linee guida in materia di protezione dei dati", corredate dagli elenchi delle minacce per Valutazione di Impatto sulla Protezione dei Dati (DPIA) e delle misure di sicurezza tecniche ed organizzative.

A relazione del Presidente Cirio:

Premesso che:

- il Regolamento (UE) 2016/679 (GDPR) approvato il 27 aprile 2016 entrato ufficialmente in vigore in tutti gli Stati membri il 25 maggio 2018, 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) stabilisce che, per la protezione dei diritti e delle libertà fondamentali delle persone fisiche, si debba assicurare un'applicazione coerente e omogenea delle norme a protezione dei dati personali, basandosi sul principio di responsabilizzazione (accountability).

- il principio di responsabilizzazione, di cui all'art. 5 del Regolamento (accountability), attribuisce direttamente al Titolare del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali, verificando che i dati vengano trattati secondo "liceità, correttezza e trasparenza"; raccolti per "finalità determinate, esplicite e legittime"; adeguati, pertinenti e limitati rispetto alle finalità; esatti; limitati nella conservazione, garantendo sicurezza e integrità;

- considerato che il Titolare, prima di procedere al trattamento dei dati, deve effettuare la valutazione d'impatto sulla protezione dei medesimi (DPIA) nel caso di trattamenti che comportano un rischio elevato per i diritti e le libertà delle persone fisiche e, conseguentemente mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al Regolamento (art. 24).

Dato atto che:

- stante la particolare complessità delle azioni da porre in essere da parte di tutte le strutture regionali, con d.d. n. 74 del 3 aprile 2019 è stato istituito il Gruppo di lavoro interdirezionale GDPR per il coordinamento delle attività necessarie per il recepimento della normativa privacy e la risoluzione di problematiche complesse legate agli adempimenti connessi all'applicazione del nuovo quadro di regole previste dal Regolamento sopra citato (GDPR);

- con D.G.R. N. 1-6847 del 18.5.2018 sono stati recepiti i primi adempimenti in attuazione del Regolamento (UE) 2016/679 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);

- con D.G.R. N. 1-7574 del 28.9.2018 sono stati designati gli incaricati, adottate le istruzioni operative e le disposizioni procedurali in materia di incidenti di sicurezza e di violazione di dati personali ed adozione del relativo registro (Data Breach) e matrice RACI;

ritenuto necessario da parte della Giunta regionale (Titolare delle attività di trattamento) dare indicazioni omogenee e uniformi per assolvere all'adempimento dei principi "di privacy by design" e "privacy by default" e per consentire una corretta valutazione di impatto sulla protezione dei dati personali (Data Protection Impact Assessment);

ritenuto, quindi, di approvare le "Linee guida in materia di protezione dei dati", in attuazione del Regolamento (UE) 2016/679, corredate dagli elenchi delle minacce per DPIA con relativa classe di rischio e delle misure di sicurezza tecniche ed organizzative, allegate alla presente deliberazione per farne parte integrante e sostanziale, da applicare alle attività che fanno capo alle strutture organizzative ed agli Uffici di comunicazione della Giunta regionale che comportano il trattamento

dei dati personali per mezzo di supporti cartacei e non, di processi manuali e/o con l'ausilio di sistemi informativi;

visto il Regolamento generale sulla protezione dei dati 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;

vista la legge regionale N. 23 del 28 luglio 2008;

attestata la regolarità amministrativa del presente provvedimento ai sensi della D.G.R. N. 1-4046 del 17.10.2016;

attestata l'assenza degli effetti diretti ed indiretti, del presente provvedimento, sulla situazione economico-finanziaria e sul patrimonio regionale, ai sensi della D.G.R. N. 1-4046 del 17.10.2016;

tutto quanto premesso e considerato, la Giunta regionale, a voti unanimi resi nelle forme di legge;

delibera

di approvare, in attuazione dell'art. 35 del Regolamento (UE) 2016/679 le "Linee guida in materia di protezione dei dati", corredate dagli elenchi delle minacce per Valutazione di Impatto sulla Protezione dei Dati (DPIA) e delle misure di sicurezza tecniche ed organizzative, allegate alla presente deliberazione per farne parte integrante e sostanziale, da applicare alle strutture organizzative e agli Uffici di comunicazione della Giunta regionale;

di dare atto che il presente provvedimento non comporta oneri a carico del bilancio regionale.

La presente deliberazione sarà pubblicata sul B.U. della Regione Piemonte ai sensi dell'art. 61 dello Statuto e dell'art. 5 della L.R. 22/2010.

(omissis)

Allegato

ADEMPIMENTI PRIVACY

Linee guida in materia di protezione dati

Regolamento (UE) 2016/679 "Regolamento Generale sulla Protezione dei Dati" (GDPR 2016/679)

-.

I. LA TUTELA ATTRAVERSO LA PROGETTAZIONE ED ATTRAVERSO L'IMPOSTAZIONE PREDEFINITA (PRIVACY BY DESIGN e BY DEFAULT).

II. ATTIVITA' DI TRATTAMENTO E VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI (DATA PROTECTION IMPACT ASSESSMENT).

1. Premessa ed ambito di applicazione

Finalità del documento, che integra la DGR n. 1-7574 del 28/09/2018, è di illustrare gli ulteriori principi/adempimenti introdotti dalla nuova disciplina in materia di protezione dei dati personali (Regolamento UE 2016/679 "Regolamento Generale sulla Protezione dei Dati" nel seguito GDPR), al fine del loro recepimento da parte dell'amministrazione regionale.

In particolare, si applica alle attività che fanno capo alle Strutture organizzative ed agli Uffici di comunicazione della Giunta regionale che comportano il trattamento dei dati personali per mezzo di supporti cartacei e non, di processi manuali e/o con l'ausilio di sistemi informatici. Sono, pertanto, escluse dall'ambito di applicazione delle presenti linee guida le attività amministrative che non contemplano trattamento di dati personali (a titolo di esempio i servizi ed i processi che comportano il trattamento di dati tecnici o di tipo statistico o aggregato, l'attività amministrativa preordinata all'adozione di testi normativi). Non si applicano, altresì, ai trattamenti di cui sono titolari il Consiglio regionale, gli Enti strumentali della Regione, le società a partecipazione regionale, gli Enti del Sistema Sanitario Regionale, in quanto dotati di propria autonomia rispetto ai processi ed all'organizzazione per la conformità alla normativa in materia di trattamento dati.

Nel caso di esternalizzazione di servizi da parte degli Uffici regionali, le presenti indicazioni dovranno essere considerate ai fini della progettazione e sviluppo delle attività e recepite all'interno degli accordi contrattuali o convenzionali.

2. Glossario

- **Accountability**: “responsabilizzazione” dei Titolari e Responsabili del Trattamento, nell’adottare proattivamente comportamenti tali da dimostrare l’adozione di misure concrete per assicurare l’applicazione del GDPR.
- **Cifratura**: misura di sicurezza che rende incomprensibili i dati personali a chiunque non sia autorizzato ad accedervi, se non con una chiave di cifratura predisposta.
- **Data Protection Impact Assessment (DPIA)**: attività di valutazione delle conseguenze che il trattamento dei dati potrebbe arrecare ai diritti e alle libertà dei soggetti cui i dati si riferiscono. In funzione dell’esito della valutazione vengono definite misure di sicurezza proporzionate al rischio del trattamento per mitigarlo in misura adeguata.
- **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 ad 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.
- **Dato personale giudiziario**: dato personale relativo alle condanne penali e ai reati o a connesse misure di sicurezza.
- **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.
- **DPO**: è il responsabile della protezione dei dati. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all’interno dell'ente, affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.
- **GDPR**: General Data Protection Regulation UE 2016/679, il nuovo Regolamento generale sulla protezione dei dati, pubblicato il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, efficace dal 25 maggio 2018.
- **Interessato**: la persona fisica cui si riferiscono i dati personali.
- **Minimizzazione**: i dati raccolti sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
- **Misure di sicurezza**: misure tecniche e organizzative per garantire la protezione dei dati personali.

- **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.
- **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 conservate 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 (art.4, par. 1, GDPR).
- **Registro dei trattamenti***:* registro delle attività di trattamento svolte sotto la responsabilità del titolare del trattamento o per conto del titolare da parte di un soggetto terzo.
- **Responsabile***:* la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
- **Scoring**: modelli di previsione delle insolvenze che si fondano su metodologie di carattere statistico. Tali modelli consentono una valutazione automatica delle aziende sottoposte ad analisi, fornendo per ognuna di esse uno score, cioè un numero (ricavabile dall'inserimento nel modello di alcuni indicatori (indici di bilancio, informazioni Centrale Rischi, dati andamentali) atto a riclassificare le stesse in categorie di aziende sane e rischiose.
- **Titolare**: 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 siano 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.
- **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.

I. LA TUTELA ATTRAVERSO LA PROGETTAZIONE ED ATTRAVERSO L'IMPOSTAZIONE PREDEFINITA (PRIVACY BY DESIGN e BY DEFAULT).

Il GDPR ha introdotto due nuovi concetti/principi: **privacy by design** e **privacy by default**.

Il primo, **"privacy by design"**, esprime l'esigenza di tutelare il dato sin dalla fase di progettazione. Si tratta di una progettazione *ex ante* che deve essere delineata dal titolare del trattamento che agisce assumendosi la responsabilità del progetto di sicurezza dei dati. Il titolare, quindi, in base al fondamentale principio introdotto dal legislatore europeo, ossia quello di responsabilizzazione (*accountability*), diventa attore, assumendosi *ex ante* la responsabilità delle misure di sicurezza che ritiene idonee alla luce dell'esito dell'analisi del rischio effettuata.

Il secondo "**privacy by default**", esprime la necessità di tutela dei dati come impostazione predefinita dell'organizzazione dell'ente. Tale principio impone al Titolare di attuare specifiche misure tecniche e organizzative al fine di garantire la massima protezione dei dati raccolti attraverso il loro minimo e indispensabile trattamento, ristretto al solo raggiungimento della finalità per la quale sono stati rilasciati.

I corollari dei principi di **privacy by design e privacy by default** sono quindi i seguenti:

- **prevenire e non correggere**: i rischi privacy vanno valutati nella fase di progettazione e qualunque sistema o processo deve essere progettato in modo tale da prevenire eventi negativi e rischio di violazione dei dati personali (proattivo, non reattivo);
- **privacy per impostazione predefinita**: il sistema deve essere progettato per garantire la massima protezione possibile dei dati personali dell'utente, senza necessità per quest'ultimo di attivarsi per ottenere tale risultato;
- **privacy incorporata nella progettazione**: le misure a protezione dei dati personali devono essere incluse nel sistema dal punto di vista progettuale e architetturale, quali sue componenti essenziali;
- **massima funzionalità**: il sistema deve soddisfare tutti gli obiettivi e gli interessi in gioco;
- **sicurezza "end-to-end"**: protezione durante tutto il ciclo di vita del dato;
- **visibilità e trasparenza**: tutte le fasi del trattamento devono essere trasparenti in modo che sia verificabile l'effettiva protezione dei dati rispetto agli obiettivi e alle finalità dichiarate dal titolare del trattamento;
- **centralità dell'utente**: il sistema deve garantire il rispetto dei diritti dell'interessato e la loro effettività, fornendo all'utente strumenti adeguati a tal fine.

Applicazione del principio di privacy by design e privacy by default

Come sopra rilevato, il rispetto del principio di *privacy by design e privacy by default* esige che le Strutture regionali valutino, sin dall'inizio della progettazione di un'attività o delle relative modifiche sostanziali, l'esigenza di tutela dei dati personali oggetto di trattamento attraverso la definizione *ex ante* di prescrizioni e strumenti anche informatici idonei a garantire il rispetto delle previsioni del GDPR e, dunque, la migliore protezione dei dati personali oggetti di trattamento.

Si applica in tutti i casi in cui viene attivato un nuovo processo/procedimento/servizio/progetto o quando vengono introdotte modifiche significative ai processi/procedimenti/servizi/progetti esistenti e ai relativi trattamenti di dati.

In particolare, si fa riferimento alle seguenti casistiche ove sia previsto un trattamento di dati personali:

1) nuovi processi/procedimenti amministrativi (a titolo esemplificativo bandi, procedure d'appalto per lavori, servizi e beni, procedimenti che derivano da nuove competenze, etc.);

2) procedimenti amministrativi esistenti rispetto ai quali è intervenuta una modifica significativa relativamente alle modalità con cui i dati personali sono trattati;

3) nuovi progetti o servizi gestiti tramite piattaforme informatiche;

4) nuovi progetti o servizi gestiti tramite supporti cartacei;

5) progetti o servizi esistenti, gestiti da piattaforme informatiche o in modalità cartacea, che abbiano subìto significativi interventi e che abbiano conseguentemente modificato le modalità con cui i dati personali sono trattati.

Modifiche significative alle modalità con le quali sono trattati i dati, si possono verificare in occasione dell'introduzione di innovazioni tecnologiche (ad esempio web app, mobile app) o nuove tecnologie per l'autenticazione, modifiche riguardanti il trattamento di nuove categorie di dati personali, nuove categorie di soggetti interessati al trattamento, nuovi trasferimenti a terzi dei dati. In ciascuno di questi casi il livello di rischio per i diritti dei soggetti interessati può subire un incremento sostanziale.

Obblighi ed adempimenti in materia di sicurezza e di garanzia nei confronti dei diritti dell'interessato

A) Obblighi e adempimenti in materia di sicurezza.

Per una efficace valutazione dei rischi attinenti alla sicurezza del trattamento occorre prendere in considerazione tutte le possibili minacce a cui potrebbero essere esposti i dati trattati per adottare le misure organizzative e tecniche più adeguate a contrastarle.

A. 1) Individuazione delle minacce

Al fine di individuare misure di sicurezza adeguate è necessario individuare le possibili e potenziali minacce e le loro eventuali conseguenze.

La minaccia è un evento che potrebbe danneggiare e/o compromettere un'attività, un sistema o uno strumento di lavoro. Si parla invece di vulnerabilità, in riferimento ad un difetto nella sicurezza di una o più parti di un sistema che rende possibile una minaccia.

Altro concetto rilevante è quello di attacco, inteso come un tentativo da parte di un soggetto di sfruttare una vulnerabilità mentre il rischio è la probabilità di essere bersaglio.

La contromisura (o misura) è un'azione o uno strumento che contrasta una minaccia e ne mitiga il rischio.

I processi di identificazione, analisi e valutazione delle minacce e delle vulnerabilità rappresentano lo strumento per comprendere e misurare l'impatto del rischio e, di conseguenza, per decidere in merito alle misure da implementare per mitigarlo e gestirlo.

Al fine di meglio qualificare la pericolosità di un eventuale attacco, effettuando una valutazione del rischio relativo al verificarsi di un determinato evento, stimandone al contempo le eventuali conseguenze, è stato definito un elenco di possibili minacce.

Tale elenco, a supporto dell'attività lavorativa, necessita di un periodico aggiornamento poiché le minacce possono, con il tempo, essere superate mentre nuove e ulteriori minacce potrebbero manifestarsi successivamente.

A 2) Predisposizione delle misure di sicurezza

L'art. 5, par. 1, lett. f), del GDPR stabilisce che i dati personali devono essere *"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"*.

E' importante notare che la protezione dei dati deve essere garantita per tutta la durata dell'attività di trattamento, includendo anche la relativa fase della conservazione dei dati stessi.

L'art. 32 del GDPR fissa alcuni principi fondamentali in materia di sicurezza richiedendo che, in particolare, le misure di sicurezza siano approntate *"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*".

Tale disposizione esige che le misure di sicurezza da adottare comprendano tra le altre:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

L'esigenza di sicurezza assume rilievo sia sotto l'aspetto informatico del trattamento sia sotto l'aspetto organizzativo, al fine di mitigare il rischio di eventi quali la sottrazione o la perdita di documenti. L'attuazione delle misure di sicurezza, quindi, dovrà garantire che:

- i dati possano essere consultati, modificati, divulgati o cancellati solo dalle persone autorizzate a farlo (e che tali persone agiscano solo nell'ambito dell'autorità che gli viene concessa);
- i dati trattati siano accurati e completi in relazione al motivo per cui sono elaborati;
- i dati rimangano accessibili e utilizzabili, cioè, in caso di perdita, modifica o distruzione accidentale, si sia in grado di recuperarli e prevenire danni alle persone interessate, predisponendo un opportuno piano di continuità operativa.

L'efficacia delle misure di sicurezza viene valutata, all'interno dell'ente, tramite audit periodici, tecnologici, documentali e organizzativi.

Sono stati predisposti gli elenchi qui contenuti indicandi misure di sicurezza tecniche (comprensive delle misure minime previste da Agid) e organizzative; tali misure verranno introdotte e rese disponibili all'interno della procedura informatica per la composizione del registro dei trattamenti di cui al punto A.3) Come osservato per le "minacce", anche l'elencazione delle misure di sicurezza non deve essere intesa quale strumento statico ed esaustivo, potendo subire variazioni ed integrazioni.

A.3) Il registro trattamenti

L'art. 30 del GDPR prevede, tra gli adempimenti principali, la tenuta del registro delle attività di trattamento. E' un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare e dai responsabili del trattamento: esso costituisce uno dei principali elementi di *accountability* in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno dell'ente, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il Registro dei trattamenti è un importante strumento di censimento e analisi dei trattamenti effettuati dal Titolare. In quanto tale, il registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento. Al riguardo si precisa che:

- nel campo "**finalità del trattamento**" (*i dati personali sono raccolti per finalità determinate, esplicite e legittime*), occorre esplicare quali siano le finalità distinte per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini);
- nel campo "**basi giuridiche che legittimano il trattamento**" occorre specificare che il trattamento è lecito in quanto ricorre almeno una delle seguenti condizioni: adempimento di un obbligo legale del Titolare, consenso libero e informato, esecuzione di un compito di interesse pubblico, esecuzione di un contratto di cui l'interessato è parte, salvaguardia degli interessi vitali dell'interessato, salvaguardia di un'altra persona fisica, trattamento necessario per il perseguimento di un legittimo interesse del Titolare (art. 6 GDPR);
- nel campo "**riferimenti normativi e legittimi interessi**", occorre indicare la base normativa del trattamento;
- nel campo "**origine dei dati**", occorre indicare se i dati oggetto del trattamento sono stati raccolti presso l'interessato o comunicati da terzi;
- nel campo "**tipo di banca dati**", occorre indicare se il trattamento avviene in forma cartacea o automatizzata;
- nel campo "**categorie di dati**", devono essere specificate le tipologie di dati oggetto di trattamento (es. dati personali, dati particolari oppure reati e condanne penali);
- nel campo "**categorie di interessati**", occorre indicare qualsiasi persona fisica identificata o identificabile a cui si riferiscono i dati ;
- nel campo **"titolari selezionati"** occorre indicare 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;
- nel campo "r**esponsabili del trattamento",** occorre indicare la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- nel campo "**trasferimenti e comunicazioni**", devono essere riportati, anche semplicemente per categoria di appartenenza, gli altri titolari a cui sono comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi); devono inoltre, essere indicati gli eventuali trasferimenti di dati personali verso una nazione terza o un'organizzazione internazionale;

- nel campo "**misure di sicurezza**", occorre selezionare le misure tecniche trasversali e le misure di sicurezza organizzative;
- nel campo "**periodo di conservazione dei dati**", occorre indicare il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

La Giunta regionale, tramite CSI Piemonte, si è dotata di un applicativo web denominato "Data protection manager (DPM)" che consente sia il popolamento del registro dei trattamenti, sia la gestione delle valutazioni d'impatto.

Lo strumento è stato anche personalizzato nei contenuti disponibili per meglio rispondere alle esigenze dell'ente e consentire una maggiore omogeneità nella descrizione dei trattamenti delle diverse strutture

A.4) Titolare, responsabile e ruolo dei referenti interni privacy e ICT

È bene precisare che tra le misure intraprese *ex ante*, rientrano sia le misure tecniche (ad es. Pseudonimizzazione) sia quelle organizzative (ad es. Procedura per la gestione dei Data Breach) messe in atto per gestire le informazioni, la loro salvaguardia e difesa in caso di intrusioni e alterazioni non autorizzate. Infatti, vi sono anche tutte quelle misure organizzative che riguardano il sistema delle autorizzazioni relative all'accesso ai dati.

Procedendo con ordine, il sistema delle nomine appare necessario nel rispetto del principio di riservatezza inteso nel senso introdotto dal Considerando 83 del GDPR, il quale menziona esplicitamente la riservatezza come adeguato strumento di sicurezza dei dati, proprio perché l'obiettivo del Titolare deve essere quello di impedire anche l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento (cfr. Considerando 39 del GDPR).

Le designazioni consentono quindi di distribuire, sin da subito, prima che avvenga il Trattamento, le responsabilità tra Titolare e responsabile, attribuendo a quest'ultimo una serie di obblighi, affinché non solo egli operi soltanto su istruzioni del Titolare ma anche applichi una serie di misure tecniche e organizzative volte al trattamento lecito dei dati, coadiuvando così il Titolare nell'esecuzione degli obblighi a lui attribuiti.

Calando tali disposizioni generali nel sistema organizzativo della Giunta regionale, si è previsto che per ogni direzione siano individuati dei referenti privacy che forniscono supporto, all'interno della struttura di appartenenza, per le tematiche privacy, per le attività di composizione del registro dei trattamenti e nel corso della valutazione di impatto (DPIA).

Il DPO presta consulenza e supporto ai referenti privacy e organizza, con gli stessi, confronti sulle problematiche generali, specifici incontri di formazione e di aggiornamento, al fine di garantire la

massima omogeneità nell'interpretazione delle norme e nell'individuazione e descrizione dei trattamenti in uso presso l'ente.

Sempre nell'ottica di garantire uniformità nelle descrizioni, la competenza al caricamento dei dati sullo specifico applicativo è attribuita esclusivamente ai referenti privacy e ai referenti ICT (Information, communication, tecnology) di direzione che provvedono alla compilazione dei campi per la composizione del registro dei trattamenti e per la valutazione di impatto (DPIA) secondo le indicazioni fornite dai responsabili delle Strutture.

Responsabile della descrizione del trattamento, ai fini del registro e della Valutazione di impatto, rimane il dirigente responsabile della struttura (Settore, Struttura temporanea, o, nel caso di coinvolgimento di più strutture interne, la Direzione) cui il trattamento afferisce.

E', pertanto, necessario che resti documentata la validazione, da parte del dirigente responsabile, delle informazioni inserite dal referente privacy, sia in fase di primo caricamento che in fase di eventuali successive modifiche.

A.5) Procedura per la gestione dei Data Breach - rinvio

Per quanto riguarda le disposizioni procedurali in materia di incidenti di sicurezza e di violazioni dei dati personali e adozione del relativo registro (data breach) si rinvia a quanto disciplinato dalla DGR 1-7574 del 28/09/2018.

A.6) Policy

Le politiche (policy, procedure, linee guida interne, circolari), a loro volta, vanno annoverate tra le misure organizzative che implementano la protezione dei dati sin dalla progettazione di prodotti, servizi o applicazioni, in quanto consentono di modellare il Trattamento dei Dati Personali su regole prestabilite.

A.7) Formazione

Occorre valorizzare la formazione di ogni persona autorizzata a trattare i dati personali, che ricade tra le misure di natura organizzativa, grazie alla quale è possibile assicurarsi che chi materialmente tratta i Dati Personali per conto dell'Ente conosca regole e potenziali rischi di tale attività.

B) <u>obblighi e adempimenti di garanzia nei confronti dei diritti dell'Interessato</u>

B.1) Nomina del Data Protection Officer (DPO) - rinvio

La nomina di un responsabile per la protezione dei dati (DPO) costituisce una misura organizzativa che consente di rispettare il principio di *data protection-by-design e di data protection-by-default*, in

quanto tale figura svolge diversi compiti tra cui la sorveglianza sull'applicazione del GDPR da parte dell'Ente e sul rispetto «*delle politiche del titolare del trattamento o del responsabile*». La sua funzione è proprio quella di garantire l'implementazione della protezione dei dati *ab origine*, assicurando agli Interessati una tutela che va oltre la semplice applicazione della norma, grazie alla maggiore consapevolezza del Titolare e dei Responsabili rispetto ai rischi del Trattamento e agli strumenti per mitigarli.
La nomina del DPO per la Giunta regionale è avvenuta con la DGR n. 1-6847 del 18/05/2018.

B.2) Diritti degli interessati

Il Regolamento UE dedica l'intero Capo III ai diritti dell'interessato ed in particolare:

art. 12 - Trasparenza e modalità attraverso le quali l'interessato viene messo a conoscenza di come può esercitare i suoi diritti;

art. 13 e 14 - Le informazioni che devono essere fornite all'interessato e le relative modalità;

art. 15 - I diritti di accesso dell'interessato alla conoscenza di quali dati che a lui si riferiscono sono in possesso del titolare, i relativi trattamenti e quanto a questi è correlato in termini di misure di sicurezza;

art. 16 - Il diritto di rettifica;

art. 17 - Il diritto alla cancellazione (oblio);

art.18 - Il diritto di limitazione del trattamento;

art.19 - Obbligo di notifica da parte del Titolare all'interessato in caso di rettifica, cancellazione, limitazioni;

art. 20 - Portabilità dei dati;

art. 21 - Opposizione al proseguimento di un trattamento;

art. 22 - L'interessato ha il diritto di non essere sottoposto ad un processo automatizzato che produca effetti giuridici che lo riguardano o che incida sulla sua persona, salvo i casi previsti al comma 2 dello stesso articolo.

I diritti richiamati, a norma dell'art. 23 (C73) e per le motivazioni espresse nello stesso articolo, possono subire limitazioni.

In estrema sintesi, il processo prevede l'informazione preventiva all'interessato (cfr DGR n. 1-7574 del 28/09/2018 che contiene, in allegato, l'informativa da adeguare al caso specifico) e la richiesta del consenso, ove applicabile, quali misure antecedenti l'avvio del trattamento con riguardo ad una

persona fisica e il diritto della stessa di poter intervenire, con modalità certe e tempi definiti, nell'ambito dei trattamenti e relativi dati che lo riguardano, sia per acquisirne la conoscenza sia per richiedere eventuali misure fra quelle previste dal Regolamento.

Al fine di facilitare ulteriormente l'esercizio dei diritti degli interessati ed anche allo scopo di considerare correttamente tali diritti nel momento in cui viene effettuata una valutazione di impatto, si ritiene utile riportare di seguito alcune definizioni e le modalità con cui i diritti possono essere esercitati nell'ambito della Giunta regionale:

Accesso. Il diritto di accesso può essere esercitato contattando il Responsabile della protezione dati (DPO) agli indirizzi: dpo@cert.regione.piemonte.it e dpo@regione.piemonte.it utilizzando apposita modulistica reperibile sul sito istituzionale https://www.regione.piemonte.it/web/ e allegando un documento di riconoscimento. Il DPO provvederà all'inoltro della richiesta al delegato del Titolare del trattamento (tramite e-mail) affinché venga fornita risposta all'interessato entro 30 giorni dal ricevimento della richiesta. Il DPO ha facoltà di effettuare controlli dell'avvenuta evasione della richiesta, monitorandone la procedura. La richiesta verrà registrata dal delegato del Titolare in apposito registro denominato "Richieste degli interessati" in una specifica area del DPM.

Rettifica. Il diritto di rettifica può essere esercitato contattando il Responsabile della protezione dati (DPO) agli indirizzi: dpo@cert.regione.piemonte.it e dpo@regione.piemonte.it utilizzando apposita modulistica reperibile sul sito istituzionale https://www.regione.piemonte.it/web/ e allegando un documento di riconoscimento. Il DPO provvede all'inoltro della richiesta al delegato del Titolare del trattamento (tramite e-mail) affinché venga fornita risposta all'interessato entro 30 giorni dal ricevimento della richiesta. Il DPO ha facoltà di effettuare controlli dell'avvenuta evasione della richiesta, monitorando la procedura. La richiesta è registrata dal delegato del Titolare in apposito registro denominato "Richieste degli interessati" in una specifica area del DPM.

Cancellazione. Il diritto alla cancellazione non può essere sempre esercitato. Il rifiuto della cancellazione da parte del Titolare del trattamento può essere giustificato quando il trattamento sia necessario per l'esercizio del diritto alla libertà di espressione e di informazione, oppure avvenga nell'adempimento di un obbligo giuridico previsto dal diritto dell'Unione o degli Stati membri, oppure sia motivato dall'interesse pubblico nel settore della sanità pubblica, oppure abbia finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o fini statistici, oppure infine sia necessario per l'esercizio o la difesa di un diritto in sede giudiziaria. Il diritto di cancellazione può essere esercitato contattando il Responsabile della protezione dati (DPO) agli indirizzi: dpo@cert.regione.piemonte.it e dpo@regione.piemonte.it utilizzando apposita modulistica

reperibile sul sito istituzionale https://www.regione.piemonte.it/web/ e allegando un documento di riconoscimento. Il DPO provvederà all'inoltro della richiesta al delegato del Titolare del trattamento (tramite e-mail) affinché sia fornita risposta all'interessato entro 30 giorni dal ricevimento della richiesta. Il DPO ha facoltà di effettuare controlli dell'avvenuta evasione della richiesta, monitorando la procedura. La richiesta è registrata dal delegato del Titolare in apposito registro denominato "Richieste degli interessati" in una specifica area del DPM.

- **Portabilità.** Difficilmente possono esistere casi di portabilità presso la Giunta regionale. Il diritto di portabilità può essere, comunque, esercitato contattando il Responsabile della protezione dati (DPO) agli indirizzi: dpo@cert.regione.piemonte.it e dpo@regione.piemonte.it utilizzando apposita modulistica reperibile sul sito istituzionale https://www.regione.piemonte.it/web/ e allegando un documento di riconoscimento. Il DPO provvede all'inoltro della richiesta al delegato del Titolare del trattamento (tramite e-mail) affinché sia fornita risposta all'interessato entro 30 giorni dal ricevimento della richiesta. Il DPO ha facoltà di effettuare controlli dell'avvenuta evasione della richiesta, monitorando la procedura. La richiesta è registrata dal delegato del Titolare in apposito registro denominato "Richieste degli interessati" in una specifica area del DPM.

- **Opposizione.** Il diritto di opposizione da parte dell'interessato può essere esercitato in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'art. 6, paragr. 1, lett. e) o f) GDPR. Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi (art. 21, par. 1, GDPR). Il diritto di opposizione può essere esercitato contattando il Responsabile della protezione dati (DPO) agli indirizzi: dpo@cert.regione.piemonte.it e dpo@regione.piemonte.it utilizzando apposita modulistica reperibile sul sito istituzionale https://www.regione.piemonte.it/web/ e allegando un documento di riconoscimento. Il DPO provvede all'inoltro della richiesta al delegato del Titolare del trattamento (tramite e-mail) affinché sia fornita risposta all'interessato entro 30 giorni dal ricevimento della richiesta. Il DPO ha facoltà di effettuare controlli dell'avvenuta evasione della richiesta, monitorandone la procedura. La richiesta è registrata dal delegato del Titolare in apposito registro denominato "Richieste degli interessati" in una specifica area del DPM.

II ATTIVITA' DI TRATTAMENTO E VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI (DATA PROTECTION IMPACT ASSESSMENT):

1. Le previsioni del GDPR.

La Valutazione d'impatto sulla protezione dei dati rappresenta una delle principali novità introdotte dal Regolamento europeo in materia di dati personali 2016/679 (GDPR, General Data Protection Regulation) in quanto correlata al principio generale di responsabilizzazione del Titolare del trattamento (*accountability*).

La Valutazione di impatto sulla protezione dei dati personali (nel seguito DPIA) è un processo che permette di valutare il livello di esposizione al rischio associato al trattamento dei dati personali e la necessità e proporzionalità del trattamento medesimo al fine di garantire e dimostrare la conformità dell'attività di trattamento con le prescrizioni del GDPR.

L'art. 35 del GDPR impone al Titolare di effettuare la DPIA prima di iniziare una data attività di trattamento che possa comportare *"un rischio elevato per i diritti e le libertà delle persone"*, in particolare quando prevede di avviare un trattamento mediante *"utilizzo di nuove tecnologie, avuto riguardo alla natura, all'oggetto, al contesto e alle finalità del trattamento"*.

La DPIA può avere ad oggetto un singolo trattamento o un insieme di trattamenti simili, che presentano rischi elevati analoghi.

L'art. 35 del GDPR individua, a titolo esemplificativo e non esaustivo, le seguenti tipologie di attività di trattamento a probabile *"rischio elevato"*:

> *"a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
>
> *b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10 alla sorveglianza sistematica su larga scala di una zona accessibile al pubblico;*
>
> *c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico"*.

Il GDPR non definisce il concetto di *"rischio elevato"* nè il concetto di *"larga scala";* ciò nondimeno vari "Considerando" del GDPR introducono elementi utili a comprendere se una data attività di trattamento sia suscettibile di comportare "*un rischio elevato per i diritti e le libertà delle persone"*.

In linea generale il GDPR aiuta a comprendere come le casistiche di rischio possano avere probabilità e gravità diverse e derivare da attività di trattamento suscettibili di arrecare pregiudizi fisici, materiali o immateriali, in particolare se il trattamento possa comportare *"discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo",* la perdita di controllo da parte dell'interessato sui dati personali che li riguardano o privazioni o limitazioni nell'esercizio dei propri diritti fondamentali e libertà (v. Considerando 75 del GDPR).

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate avendo riguardo *"alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento"* (v. Considerando 76 del GDPR).

Dunque, occorrerà valutare se il trattamento riguardi "*dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza"* o sia finalizzato a valutare aspetti personali *"in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali"* o se si riferisca a *"dati personali di persone fisiche vulnerabili, in particolare minori"* o se riguardi *"una notevole quantità di dati personali e un vasto numero di interessati*" (v. Considerando 75 del GDPR).

Con riferimento ai trattamenti *"su larga scala",* ossia relativi ad una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potenzialmente presentano un rischio elevato, il GDPR incentra l'attenzione sulle categorie di dati particolari o sulle finalità delle attività di trattamento *"per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza."* (v. Considerando 91 del GDPR).

Un esempio di attività da sottoporre a DPIA è rinvenibile nell'ipotesi in cui "*autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di*

trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata" (v. Considerando 92 del GDPR).

Per contro *"non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati*." (v. Considerando 91 del GDPR).

Infine, particolare attenzione deve essere posta su quei trattamenti che "*comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale"* (v. Considerando 89 del GDPR).

Qualora l'esito della DPIA escluda la sussistenza di un rischio elevato, il Titolare può ritenersi legittimato ad eseguire il trattamento, in caso contrario, non potrà attivare il trattamento senza prima aver adottato le misure idonee a garantire un livello di sicurezza adeguato ai rischi per attenuarli o eliminarli.

Nell'ipotesi residuale in cui il Titolare non sia in grado di individuare dette misure tecniche od organizzative dovrà allora consultare l'Autorità di controllo, ai sensi dell'art. 36 del GDPR, dando luogo alla c.d. consultazione preventiva.

Il GDPR demanda alle Autorità di controllo di ogni Stato membro la predisposizione di un elenco di tipologie di attività per le quali è obbligatoria la DPIA e un elenco di attività escluse (v. art. 35 par. 4 e 5 del GDPR).

2. Le tipologie di trattamenti di dati individuate dal Garante italiano.

In attuazione del GDPR, il Garante Privacy italiano, con provvedimento n. 467 dell'11 ottobre 2018, ha approvato un elenco di 12 tipologie di attività di trattamento dei dati per le quali è obbligatorio effettuare la DPIA.

L'elenco pubblicato trae origine non solo dalle previsioni del GDPR ma anche dai nove criteri elaborati dal Gruppo di lavoro "Articolo 29" nelle apposite Linee Guida in materia di Valutazione d'impatto adottate il 4 aprile 2017 ed emendate il 4 ottobre 2017 (v. Linee Guida WP n. 248, rev. 01).

Ha natura vincolante ma non esaurisce le tipologie di attività di trattamento che potrebbero presentare un *"rischio elevato":* per tale ragione il Garante privacy rimarca la necessità di osservare i contenuti delle Linee Guida WP n. 248, rev. 01, in quanto forniscono un valido strumento orientativo in ordine alla scelta di effettuare o meno una DPIA [1].

Giova, inoltre, evidenziare come, nei casi di incertezza sulla sussistenza di un rischio elevato, il Gruppo di lavoro "Articolo 29" raccomandi di effettuare la DPIA, poichè tale valutazione consente di dimostrare il grado di conformazione al GDPR.

Di seguito si riportano le dodici tipologie di trattamento individuate dal Garante privacy:

1. trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"* [2];

2. trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi);

3. trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti,

1 Si riportano i 9 criteri illustrati nelle Linee Guida WP n. 248 rev. 01 e richiamati dal Garante Privacy: 1) valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato; 2) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente; 3) monitoraggio sistematico degli interessati (ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico); 4) il trattamento di dati sensibili o dati aventi carattere altamente personale (v. artt. 9 e 10 del GDPR); 5) il trattamento di dati su larga scala; 6. creazione di corrispondenze o combinazione di insiemi di dati; 7) il trattamento di dati relativi a interessati vulnerabili (v. considerando 75 del GDPR). Ciò comporta uno squilibrio di potere tra gli interessati e il titolare del trattamento, minando o impedendo la possibilità di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti; 8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative (es. la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici); 9. quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (v. art. 22 e considerando 91 del GDPR). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto (es. una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno).

2 Per un approfondimento sul concetto di profilazione si rinvia alle Linee Guida sul processo decisionale automatizzato relativo alle persone fisiche WP n. 251 del 6 febbraio 2018.

effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati, ad es. in ambito telecomunicazioni, banche, effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza;

4. trattamenti su larga scala di dati aventi carattere estremamente personale (v. Linee Guida WP n. 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti);

5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (v. quanto stabilito dalle Linee Guida WP n. 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8);

6. trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);

7. trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nelle Linee Guida WP n. 248, rev. 01;

8. trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;

9. trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);

10. trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

11. trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento; [3]

12. trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Il Garante privacy ha chiarito come le espressioni trattamenti *"sistematici"* e *"non occasionali"*, indicate nell'elenco delle tipologie di trattamenti, siano riconducibili al criterio della *"larga scala"* illustrato nelle Linee Guida WP n. 248, rev. 01. Al proposito, il Gruppo articolo 29 WP29 raccomanda di porre particolare attenzione ai seguenti fattori: il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata dell'attività di trattamento; l'estensione geografica dell'attività di trattamento.

Alla luce del suddetto quadro normativo e interpretativo, emerge come l’applicazione di un processo DPIA sia da ritenere obbligatoria ogni qualvolta si riscontri un trattamento che, in ragione della tipologia di dati trattati (ad es. dati sanitari o giudiziari), della categoria degli interessati (ad es. soggetti vulnerabili), delle modalità di trattamento (es. mediante l'uso di nuove tecnologie o la profilazione degli interessati) e delle finalità (es. elaborare dati personali per valutare i comportamenti degli interessati), comporti un rischio elevato per i diritti e le libertà delle persone fisiche.

3 Si riporta la definizione del GDPR di «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.

ELENCO MINACCE PER DPIA CON RELATIVA CLASSE DI RISCHIO RID ADOTTATE DALLA GIUNTA REGIONALE

Categoria	Codice	Minaccia	Dettagli	RID
1. Eventi inattesi con conseguenti danni fisici	M1.1	Incendio, allagamento, polvere, corrosione, congelamento		D
	M1.2	Distruzione di strumentazione, supporti, documenti	comprensivo di atti dolosi e terroristici	D
2. Eventi climatici	M2.1	Fenomeni climatici (uragani, nevicate, esondazioni)	comprende eventi legati alle scariche atmosferiche	D
	M2.2	Terremoti		D
3. Perdita di servizi essenziali	M3.1	Interruzione o non disponibilità di sistemi complementari (energia elettrica, climatizzazione…)		D
	M3.2	Malfunzionamento di infrastrutture e piattaforme	Cloud, data center…	RID
	M3.3	Interruzione o non disponibilità della rete, errori di trasmissione	comprende malfunzionamenti nei componenti di rete, danni alle linee di TLC	RID
	M3.4	Indisponibilità del personale	interruzioni o rallentamenti di servizi, processi e attività provocati dall'assenza (accidentale o deliberata) di personale	D
4. Compromissione di informazioni	M4.1	Divulgazione di informazioni	Da parte di soggetti autorizzati tenuti alla riservatezza	RD
	M4.2	Comportamenti fraudolenti dei dipendenti		RID
	M4.3	Intercettazione delle comunicazioni		R
	M4.4	Furto di documenti, supporti di memorizzazione, componenti, strumenti di lavoro	comprende il furto di server, pc, notebook, tablet, smartphone	RID
5. Problemi tecnici	M5.1	Errori/malfunzionamenti/vulnerabilità nel software utlizzato	esempio per errori di progettazione, programmazione, di installazione, di compatibilità con risorse…	RID
	M5.2	Malfunzionamento negli strumenti hardware utilizzati		RID
6. Azioni non autorizzate	M6.1	Accesso logico non autorizzato alla rete/uso non autorizzato delle applicazioni e dei servizi	- accesso non autorizzato alle applicazioni o ai dati da rete interna o da rete esterna (es un utente non autorizzato con credenziali di altro utente accede a DB o applicativo) - possibilità che un utente usi un account per scopi non autorizzati (es un interessato può vedere/modificare dati di un altro soggetto, un incaricato può modificare dati che non fanno parte del trattamento autorizzato)	RID
	M6.2	Infezioni da virus, malware.../attacchi DoS o DDoS/attacchi di ingegneria sociale per carpire informazioni o identità	Infezioni anche su strumenti “mobile”, DoS: interruzione del servizio (Denial of Service), DDoS: interruzione distribuita del servizio (Distributed Denial of Service). Comprende l’utilizzo di tecniche di phishing per furto di informazioni e credenziali	RID

7. Compromissione di funzioni	M7.1	Errori involontari da parte di personale o errori nell'utilizzo del servizio da parte degli utenti finali	esempio per poca formazione, competenza o disattenzione da parte del personale o di scarsa usabilità del servizio per errori da parte dei fruitori	RID
	M7.2	Degrado dei supporti di memorizzazione delle informazioni	degrado delle memorie di massa	ID

Legenda classi di rischio RID		
R	Riservatezza	Riservatezza dei dati: protezione dei dati trasmessi o memorizzati per garantirne la confidenzialità, evita l'intercettazione o la visione da parte di soggetti terzi non autorizzati.
I	Integrità	Integrità dei dati: garantisce la completezza e integrità dei dati intesa come garanzia che l'informazione non subisca modifiche o cancellazioni involontarie anche a seguito di malfunzionamenti o danni ai sistemi tecnologici.
D	Disponibilità	Disponibilità dei dati: garantisce l'accesso al dato nel tempo e nei luoghi previsti.

ELENCO MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
ADOTTATE DALLA GIUNTA REGIONALE PER LA PROTEZIONE DEI DATI (art 32 GDPR)

In aggiunta alle misure minime di sicurezza definite dalla circolare AGID n.2/2017 si applicano le seguenti misure di sicurezza ORGANIZZATIVE E TECNICHE TRASVERSALI sui TRATTAMENTI ASSEGNATI. Le MISURE TECNICHE VERTICALI sono specifiche per ogni trattamento e sono applicate in base ai requisiti di sicurezza richiesti per i singoli servizi dei trattamento commissionati.

tipologia di misura	misura	descrizione/esempi	CODICE
MISURE ORGANIZZATIVE	**Formazione**	Esistenza di un piano di formazione in materia di protezione dei dati per il trattamento. Esecuzione degli interventi formativi previsti	MO1
	Istruzioni per il trattamento (ex Disciplinare)	Esistenza di un documento che contenga regole da applicare per il trattamento (principi, regole da applicare nel trattamento, procedure, linee guida, manuali di organizzazione del servizio ecc..) Esistenza di procedure/istruzioni che descrivono la gestione degli incidenti che possano comportare violazione di dati personali (data breach)	MO2
	Regole di archiviazione	sono definiti la politica e i processi di gestione dell'archivio cartaceo (consegna, archiviazione, consultazione etc.)	MO3
	Modello organizzativo	regole e responsabilità a livello aziendale (es codice etico) e a livello di ruoli e responsabilità del progetto o servizio	MO4
	Audit interni	effettuazione di un audit interno sul trattamento entro 1 anno solare dalla ultima valutazione (o dalla messa in esercizio del software/attivazione del servizio)	MO5
	Audit esterni	effettuazione di un audit esterno sul trattamento entro 1 anno solare dalla ultima valutazione (o dalla messa in esercizio del software/attivazione del servizio)	MO6
	Misure contratti	predisposizione di contratti passivi che includano le clausole privacy definite a livello aziendale per il rispetto del GDPR. Clausole e condizioni di dettaglio specifiche per il trattamento	MO7
	Analisi dei rischi	Predisposione di un modello di analisi dei rischi , in particolare rischi privacy e di sicurezza	MO8
	Manuali delle Procedure	sono predisposti e aggiornati i documenti di progettazione, architettura, installazione del software utilizzato? (es vista d'insieme, documento di architettura, deploy, ..)	MO9
MISURE TECNICHE VERTICALI	**Minimizzazione della quantità dei dati personali**	rientrano misure di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati	MV1
	Profilazione	utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento).	MV2
	Autenticazione (ex autenticazione centralizzata)	utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento).	MV3
	Utilizzo di sistemi di autenticazione multifattore	E previsto l'uso di certificati digitali, PIN, o autenticazione per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa	MV4
	Gestione del ciclo di vita delle credenziali (ex scadenza credenziali)	gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati)	MV5
	Tracciabilità accessi risorse (ex tracciabilità accessi DB e audit log applicativi)	possibilità di tracciare accessi alle risorse critiche (es DB, front end e back end del servizio, share di rete critici)	MV6
	Audit log applicativi	nel DB è prevista la tracciatura dell'identificativo utente che ha inserito/modificato i dati delle tabelle e si è in grado di risalire a chi e quando ha inserito/modificato/cancellato il record	MV7
	Abilitazioni puntuali accessi DB (proxy SQL)	utilizzo di proxy SQL	MV8

	Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità)	(es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,)	MV9
	Cifratura del dato	mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.)	MV10
	Cifratura del canale	Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH	MV11
	Pseudonimizzazione	adozione di tecniche che garantiscono la non attribuzione a una persona identificata o identificabile di un dato ma consentono di identificare in un secondo momento i dati anche in maniera indiretta o da remoto (es conservando separatamente le informazioni che permettono di associare la persona al dato)	MV12
	Backup cifrati	utilizzo di sistemi per la cifratura dei backup	MV13
	Business continuity/disaster recovery	esistenza di procedure per garantire la BC e/o il DR del Trattamento	MV14
MISURE TECNICHE TRASVERSALI	**Armadi e contenitori dotati di serrature**	Conservazione sicura dei documenti cartacei e backup	MT1
	Armadi e contenitori ignifughi	Conservazione sicura dei documenti cartacei e backup	MT2
	Cassaforte ignifuga	Conservazione sicura dei documenti cartacei e backup	MT3
	Misure antincendio	Misure di protezione dei bene e dei documenti	MT4
	Sistemi di sorveglianza	Misure di controllo accessi ai locali	MT5
	Gestione delle postazioni di lavoro	Misure adottate per ridurre la possibilità che le postazioni di lavoro (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni etc.) vengano sfruttate per violare la sicurezza dei dati personali (es., ..)	MT6
	Utilizzo di infrastrutture sicure (hw e complementari)	manutenzione fisica degli apparati IT e dei sistemi complementari (es. utilizzo infrastrutture in sala CED per ospitare i servizi applicativi erogati e i dati, utilizzo di protocolli di accesso sicuri)	MT7
	Infrastrutture logiche (ex patch di sistema)	utilizzo di sistemi aggiornati (es middleware, software dei sistemi, ..)	MT8
	Antivirus	installazione di antivirus aggiornato sulle postazioni di lavoro	MT9
	DLP (Data Loss Prevention)	utilizzo di sistemi di DLP per evitare la trasmissione di dati personali o riservati dalle postazioni	MT10
	Network monitoring	strumenti di packet filtering	MT11
	Protezione anti DoS e anti DDoS	misure di protezione contro gli attacchi di tipo DoS (interruzione di servizio) e DDoS (interruzione distribuita del servizio)	MT12
	Separazione LAN	separazione LAN ambienti sviluppo, test, collaudo e produzione	MT13
	Protezione della navigazione web	utilizzo sistemi di web filtering	MT14
	VPN	utilizzo di VPN per l'accesso alle risorse da remoto	MT15
	Protezione perimetrale (firewall)	strumenti di protezione della rete	MT16
	Protezione applicativa (WAF WEB Applicatin Firewall)	strumenti di protezione degli applicativi WEB	MT17
	Gestione Log accessi privilegiati (SIEM)	strumenti per la gestione dei log dei sistema. (es log dei server dei database, dei firewall, etc) . Tali strumenti permettono di correlare su piu fonti un accadimento , es un accesso illecito da un ip , posso andare a vedere su tutti i log di tutti gli apparati tracciati cosa e avvenuto, etc)	MT18
	Backup e restore	Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup	MT19