GLOSSARIO	
Reg. 679/2016 UE (GDPR), art. 4 - Definizioni	
Testo originale inglese	Versione italiana tradotta
"Personal data": means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified directly or indirectly.	**"Dato personale":** qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato", direttamente o indirettamente […]
"Processing": means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means […]	**"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 […]
"Controller": means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data […]	**"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 […]
"Outsourcer Processor": means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller […]	**"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.
"Internal Processor" (Personal Data Handler): Staff of the Data Controller who have been given responsibility for handling Personal Data as part of their operational activities.	**"Incaricato del trattamento":** personale del Titolare del trattamento a cui è stata data la responsabilità della gestione di dati personali nell'ambito delle loro attività aziendali.
"Consent of the data subject": means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.	**"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.

PREMESSA

Il **Regolamento 679/2016 UE (GDPR)** definisce **Data Breach** *"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 da un Data Controller o da un Data Processor"* **(GDPR, art. 4, par. 12).**

Il presente documento illustra il processo attraverso il quale Dopolavoro Atac Cotral intende gestire i **Data Breach** allo scopo di ridurre al minimo il tempo di esposizione al danno, minimizzare i rischi per le persone fisiche i cui dati fossero stati eventualmente violati e proteggere la reputazione dei Data Subjects e del Brand.

Nel rispetto degli artt. 33 e 34 del GDPR qualsiasi **Data Breach** comprese le relative circostanze, le possibili conseguenze ed i provvedimenti adottati o previsti per porvi rimedio, viene debitamente documentata dall'Azienda al fine di consentire all'autorità di controllo di verificare il rispetto della normativa.

TIPOLOGIE DI DATA BREACH

I requisiti di sicurezza che possono essere oggetto di violazioni riguardano:

1. **Confidentiality**
   Violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
2. **Integrity**
   Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
3. **Availability**
   Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità o distruzione, accidentale o non autorizzata, di dati personali.

In particolari circostanze le violazioni dei requisiti di sicurezza potrebbero essere combinate tra loro.

OBBLIGHI DEL DATA CONTROLLER (GDPR, artt. 33 e34)

- Se la violazione comporta un rischio per i diritti e le libertà delle persone fisiche, il Data Controller è tenuto a **notificare il Data Breach all'Autorità Garante**, tempestivamente, al massimo entro **settantadue ore** dal momento in cui ne viene a conoscenza, allo scopo di limitare i danni a carico dei Data Subjects.
- Tra gli elementi che possono determinare **l'obbligo di notifica**, vanno annoverati, a titolo esemplificativo e non esaustivo: perdita del controllo dei dati personali dei Data Subjects; limitazione dei loro diritti; discriminazione; furto o usurpazione di identità; perdite finanziarie; decifratura non autorizzata della pseudonimizzazione; pregiudizio alla reputazione; perdita di riservatezza dei dati personali protetti da segreto professionale, qualsiasi altro danno economico o sociale significativo per la persona interessata.
- Qualora, il rischio per i diritti e le libertà delle persone fisiche fosse particolarmente elevato, oltre alla notifica, il Data Controller è tenuto a **darne comunicazione senza indugio ai Data Subjects coinvolti**, indicando nome e dati di contatto del referente aziendale presso cui ottenere maggiori informazioni.

  Poiché il GDPR prevede che Il Data Processor che viene a conoscenza di una violazione ne informi senza

ingiustificato ritardo il Data Controller, Dopolavoro Atac Cotral, prima di affidare trattamenti di dati personali a Data Processor Outsourcer si accerta preventivamente della loro capacità di gestire tempestivamente e adeguatamente gli incidenti di sicurezza, prevedendo a tale scopo idonee clausole e addendum contrattuali.

FORMAZIONE DELLE RISORSE E COSTITUZIONE DEL DATA BREACHTEAM

Al fine di adempiere correttamente agli obblighi previsti dal GDPR, Dopolavoro Atac Cotral ha disposto di:

a) provvedere alla diffusione di un adeguato livello di consapevolezza e formazione in materia di Data Breach tra le risorse autorizzate al trattamento dei dati;
b) definire ruoli e responsabilità dei Data Processor, inserendo nelle clausole e addendum contrattuali, nelle nomine e negli incarichi, garanzie per il supporto nell'attività di detection e reazione in caso di Data Breach;
c) costituire un **"Data Breach Team**", per la gestione delle crisi conseguenti alle violazioni di sicurezza;
d) prevedere una procedura per la segnalazione della violazione avvenuta o tentata da parte dei Data Processor al "**Data Breach Team**"
e) istituire un Registro aggiornato di anomalie, incidenti e violazioni dei sistemi informatici aziendali.

COMPOSIZIONE DEL DATA BREACH TEAM

Il **Data Breach Team** di Dopolavoro Atac Cotral si compone delle seguenti competenze:

a) Rappresentante della Direzione,
b) Data Protection Officier (DPO),
c) Responsabile dell'Ufficio / Processo oggetto di violazione

Il **Data Breach Team** richiederà la collaborazione del Data Processor Interno e/o Outsourcer eventualmente coinvolti nella violazione.

COMPITI DEL DATA BREACH TEAM

Non appena venuto a conoscenza dell'incidente il **Data Breach Team** si attiverà per la convocazione di un Briefing allo scopo di:

a) identificare la natura dell'incidente,
b) valutare se l'incidente ha avuto impatto sulle informazioni,
c) verificare se tra le informazioni violate vi fossero dati personali,
d) qualificare la tipologia di dati personali eventualmente coinvolti,
e) individuare e descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali ed attenuarne i possibili effetti negativi per i diritti e le libertà delle persone fisiche coinvolte e salvaguardare nel contempo la Brand Reputation,
f) convocare un Post Incident Debriefing per evidenziare le vulnerabilità riscontrate e valutare l'adozione di misure tecniche e/o procedure in grado di evitare il ripetersi di analoghe tipologie di incidenti o violazioni.

Qualora l'incidente abbia avuto un impatto su informazioni e dati personali, il **Data Breach Team** si atterrà ai seguenti criteri di valutazione, documentabili, tracciabili ed in grado di fornire evidenza nelle sedi competenti:

a) natura della violazione,
b) categorie e numero approssimativo dei dati personali violati,
c) categorie e numero approssimativo di Data Subjects coinvolti,
d) identificabilità delle persone fisiche coinvolte,
e) grado di sensibilità dei dati personali violati,
f) probabili conseguenze della violazione per i diritti e le libertà delle persone fisiche coinvolte,
g) misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e se del caso attenuarne i possibili effetti negativi.

Tutte le risultanze dell'attività del **Data Breach Team** verranno debitamente documentate ed annotate nel Registro delle anomalie per consentire all'Autorità di controllo di verificare il rispetto della normativa da parte di Dopolavoro Atac Cotral**.**