UNIONE DEI COMUNI DELLA VAL D'ENZA

Procedura di gestione e documentazione delle violazioni dei dati personali (GDPR)

Maggio 2018

INDICE

1 Introduzione

1.1 Scopo

Il presente documento contiene la Procedura di gestione delle violazioni dei dati personali (*data breach*) e lo schema del Registro delle violazioni, in attuazione del Regolamento UE 2016/679 in materia di protezione dei dati personali (GDPR).

1.2 Riferimenti

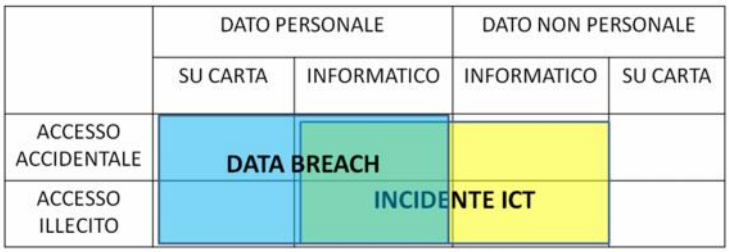
GDPR	"Regolamento UE 2016/679 in materia di protezione dei dati personali"
DBGL	"Guidelines on Personal data breach notification under Regulation 2016/679" adottate il 3/10/2017, riviste ed adottate il 6/2/2018 dal Gruppo di Lavoro Art.29
ISO27035	ISO/IEC 27035 "Information technology - Security techniques - Information security incident management"
AGID1/2017	Circolare AgID n. 2/2017 del 18 aprile 2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni"

1.3 Obblighi

Il GDPR prevede l'obbligo di notifica e comunicazione in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati: il criterio che determina l'obbligo è la probabilità che la violazione possa mettere a rischio (per la notifica all'autorità) o ad elevato rischio (per la comunicazione agli interessati) le libertà e i diritti degli individui. Più specificamente, gli artt. 33 e 34 del GDPR determinano tempi, modalità e contenuti della notifica e della comunicazione. In particolare, il comma 5 dell'art.33 obbliga a documentare le violazioni, al fine di consentire all'Autorità di verificare il rispetto del GDPR.

Le DBGL integrano il GDPR fornendo indicazioni che chiariscono una serie di domande poste dalla attuazione del GDPR.

Per le attività non espressamente prescritte da GDPR e DBGL nella presente procedura si prende ispirazione dallo standard ISO27035, che regola la gestione degli incidenti di sicurezza informatica, un dominio simile anche se non coincidente con quello del GDPR:



1.4 Il ciclo di gestione dei data breach

La gestione dei data breach richiede la definizione e messa a punto di un **sistema tecnico - organizzativo integrato**, che metta l'Ente nelle condizioni di erogare una risposta efficace alla possibile violazione dei dati personali, nel rispetto del vincolo delle 72 ore imposto dall'art. 33 comma 1 del GDPR, in un contesto verosimilmente caratterizzato da incertezze sulle informazioni disponibili e forte pressione psicologica.

Ciò richiede una significativa attività preparatoria, antecedente alle attività esecutorie descritte nel GDPR e nelle DBGL, e la periodica revisione del sistema alla luce delle "lezioni imparate" dai data breach, in una logica di miglioramento continuo.

Mutuando ed adattando il modello ISO27035, per la gestione dei data breach si prende come riferimento il seguente ciclo a tre fasi:

Fase 1	Pianificazione	Pianificazione delle attività tecniche ed organizzative
Fase 2	Esecuzione	Identificazione, valutazione, risposta, documentazione dei data breach
Fase 3	Miglioramento	Analisi periodica delle "lezioni imparate" dai data breach evitati o accaduti, e conseguente ripianificazione.

2 Attività di pianificazione

2.1 Documenti di riferimento

Documenti prodotti dalle altre attività previste dal GDPR

A monte delle preparazione del sistema di gestione dei data breach si collocano altre attività previste dal GDPR, i cui risultati sono descritti nei seguenti documenti che servono come punto di partenza per la pianificazione del sistema:

Documento	Riferimenti Documento
Nomina del titolare del trattamento dei dati (GDPR Art.24,26)	Modello organizzativo approvato con Deliberazione di Giunta n. 73/2018
Nonima dei responsabili del trattamento dei dati (GDPR Art.28)	73/2018
Nomina del DPO (GDPR Art.37-39)	73/2018
Registro delle attività di trattamento dei dati (GDPR Art.30)	BOZZA in approvazione
Analisi dei rischi di violazione o DPIA (GDPR Art.35)	BOZZA in approvazione

Documento di analisi delle misure minime di sicurezza informatica

Sempre a monte del sistema di data breach, si collocano i controlli sulle misure minime di sicurezza informatica eseguiti in ottemperanza di AGID2/2017, i cui risultati sono descritti nel modulo firmato digitalmente e custodito presso l'Ente. Mentre le analisi svolte col Registro delle attività di trattamento dei dati e DPIA seguono "verticalmente" i processi dell'Ente e possono quindi evidenziare rischi specifici dovuti alle caratteristiche del processo, le misure minime di sicurezza informatica riguardano "orizzontalmente" tutti i processi che si svolgono sui sistemi informativi dell'Ente e quindi integrano l'analisi verticale con rischi potenzialmente comuni a tutti i processi. L'assenza o il mancato raggiungimento del livello minimo delle misure previste da AGID2/2017 espongono perciò l'Ente a rischi significativi di violazione dei dati personali. Agli scopi del presente documento non sono da considerare i sistemi informativi che non trattano in alcun modo dati personali di persone viventi.

Documento	Sintesi dei risultati	Riferimenti Documento
Misure minime di sicurezza ICT (AGID2/2017)	La sintesi dei risultati dell'analisi svolta è contenuta in un documento disponibile presso i Servizi Informatici dell'Ente.	Il modulo compilato collettivamente per Unione e Comuni dell'Unione è stato approvato con Deliberazione di Giunta n. 45/2018

Procedure Operative dell'Ente

Laddove sia possibile definire attività proceduralizzate preventive (es. gestione fisica e digitale della postazione di lavoro, accesso a risorse condivise, comportamento in spazi condivisi) o da eseguirsi in caso di potenziale data breach (es. interpretazione di allarmi e di log di sistema, blocco di accessi da internet, fermo di sistemi informativi), è opportuna la stesura scritta di procedure operative, che aiutino la disseminazione di buone pratiche in tutto il personale dell'Ente e, più specificamente, accelerino l'esecuzione delle attività in caso di violazione dei dati personali minimizzando errori ed interpretazioni personali, considerando anche la situazione in cui le attività debbano essere occasionalmente svolte da personale non specializzato ma presente in sito:

Procedura Operativa relativa a	**Rivolta a**	**Riferimenti Documento**
Policy informatiche relative all'accesso, gestione password, utilizzo attrezzature.	Tutti gli utenti di Ente e Comuni	BOZZA

Nel Documento di sintesi relativo ad AGID2/2017 è disponibile un piano per la produzione di altre policy informatiche.

Repository della Documentazione

Tutti i documenti sopra elencati devono essere resi disponibili in formato digitale in un repository di facile accesso al team di gestione del data breach ed una copia cartacea deve essere custodita in un luogo noto al team, per garantire l'accesso alle informazioni in essi contenuti anche in caso di indisponibilità dei sistemi informatici:

Repository della documentazione	**Collocazione e modalità di accesso**
Digitale	Cartelle archivio Sistema Informatico Associato.
Fisico	Ufficio del Responsabile dei Servizi Generali ed Informatici.

2.2 Organizzazione del team di gestione dei data breach

Per la gestione dei data breach è necessario costituire un team, formato dalle persone che, per responsabilità o competenza, possono risultare utili nel momento del data breach. Il team è costituito dalla persona titolare del trattamento dei dati ("Titolare"), dai responsabili interni dei trattamenti dei dati ("Responsabili interni") e dagli incaricati tecnicamente competenti ad agire sui diversi sistemi coinvolti nella gestione. Il team è allargato ai Responsabili del trattamento di dati personali esterni all'Ente ("Responsabili Esterni"), se identificati dal Titolare attraverso contratti, convenzioni o altri strumenti.

Si assume per il team di gestione del data breach il modello organizzativo approvato con Deliberazione di Giunta n. 73/2018.

Per ogni figura del team è necessario valutare il livello di reperibilità necessario per rispettare il vincolo delle 72 ore nel caso peggiore (es. data breach identificato nella giornata di venerdì) e le conseguenti regole di ingaggio (giorni / orari / modalità di contatto e di azione) sostenibili dal punto di vista organizzativo ed economico. Poiché è da prevedersi il caso in cui non tutto il personale del team sia disponibile nel momento dell'evento, è opportuno definire regole di escalation (o almeno di backup) per le figure che risultassero assenti.

E' utile definire nel team il ruolo del Portavoce, incaricato di mantenere i contatti con l'Amministrazione ed eventualmente con la stampa, liberando il Titolare ed i Responsabili impegnati nelle delicate attività di analisi e valutazione e di comunicazione istituzionale con l'Autorità di Controllo.

Figura	**Interno / Esterno**	**Ruolo ed utilità in caso di data breach**	**Regole di ingaggio**	**Figura di backup**
Titolare	Interno	Coincide col Presidente dell'Unione. Rappresenta l'Ente verso l'Autorità.	E' avvisato dal Delegato in caso di evidenza di data breach.	Delegato
Delegato (nomina comunicata all'Autorità)	Interno	Coincide con il Responsabile dei Servizi Informatici / Servizi Generali. Valida la valutazione del data breach proposta dal Responsabile. Attesta il livello di rischio del data breach. Avvisa il Titolare ed il DPO. Se il caso, provvede alla notifica all'Autorità ed alle comunicazioni agli Interessati.	E' avvisato tempestivamente dal Responsabile, in caso di evidenza di data breach. Se possibile, si reca in sede.	Titolare

Figura	Interno / Esterno	Ruolo ed utilità in caso di data breach	Regole di ingaggio	Figura di backup
		Tiene le relazioni con l'Autorità. (Nota *)		
Responsabile	Interno	Coincide con il Responsabile del Settore in cui è intercettato il potenziale data breach. Partecipa alla valutazione del potenziale data breach. Se il caso, avvisa e coinvolge il Coordinatore Informatico. Propone i data breach alla validazione del Delegato.	E' avvisato tempestivamente in caso di potenziale DB. Se necessario, si reca in sede.	Delegato
Tutti i dipendenti dell'Ente	Interno	Segnalano il potenziale data breach al proprio Responsabile di Settore.	-	-

(*) Eventuali ulteriori livelli di deleghe verso i singoli Responsabili (previsti nel Modello Organizzativo approvato) saranno comunicati all'Autorità.

2.3 Formazione del team ed esercitazioni

La consapevolezza da parte del team dei rischi che l'Ente corre nella gestione dei dati è fondamentale per una corretta esecuzione delle attività di monitoraggio, identificazione e valutazione dei data breach.
Le attività di formazione del team devono quindi portare alla conoscenza ed alla comprensione non solo dei principi del GDPR ma, più concretamente, dei rischi specifici dell'Ente e delle misure messe in campo per contrastarli, attraverso una presentazione mirata dei contenuti del Registro, del DPIA e – sinteticamente - dell'analisi delle misure minime di sicurezza ICT.
La formazione teorica deve essere ripetuta (almeno in forma parziale) in seguito all'adozione di azioni di miglioramento.

Formazione su	**Ai Responsabili**	**Personale del servizio informatico e Amministrazione di sistemi esterni**	**Tutti i dipendenti**
GDPR	Effettuata	Effettuata	Da programmare
Registro attività trattamento dei dati e DPIA	Effettuata, attraverso il coinvolgimento attivo nella stesura dei documenti di analisi	In corso di valutazione	Non prevista
Procedure Operative	Da programmare	Da programmare	Da programmare, per settore
Misure minime ICT	Non prevista	Da programmare	Non prevista

Poiché l'efficace risposta ad un data breach dipende anche dalle reazioni personali in situazioni di emergenza, è opportuno accompagnare la formazione teorica con esercitazioni eseguite senza preavvisare il personale coinvolto, in cui verificare la capacità dei diversi attori di recuperare in tempi utili le informazioni necessarie e di attuare le azioni previste.

Esercitazione su	**Ai Responsabili di Settore / Trattamento**	**Struttura ICT e Amministrazione di sistemi esterni**	**Tutti i dipendenti**

Le attività di esercitazione saranno programmate al termine delle attività di formazione.

2.4 Analisi dei sistemi informatici contenenti dati personali

I sistemi informativi, i database, gli archivi non strutturati (es. share di disco) e il sistema d posta elettronica sono i principali repository dei dati personali digitalizzati e possono diventare per questo oggetto di attacchi informatici, mirati o generalizzati.
Partendo dell'analisi per processo svolta con il Registro e il DPIA e considerando lo stato evidenziato dall'analisi delle misure minime di sicurezza, si riaggregano i dati personali per sistema valutando, in analoga a quanto già effettuato per i processi, i rischi ai dati personali derivanti dalle vulnerabilità dei sistemi informatici:

SISTEMA INFORMATIVO / DATABASE / ARCHIVIO	INTERNO/ ESTERNO	CATEGORIE DI DATI PERSONALI	CATEGORIE DI SOGGETTI INTERESSATI	RISCHIO DEI PROCESSI CHE VI SI SVOLGONO	DICHIARAZIONI RELATIVE A PROTECTION BY DESIGN / BY DEFAULT
Software gestione protocollo informatico	Interno	Tutti	Tutti	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Accesso all'applicativo tramite assegnazione di profili e permessi
Documenti informatici archivio Centrale Unica di committenza	Interno	1 - 10	5 - 7	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Lista controllo accessi (ACL) cartelle archivio
Documenti informatici archivio servizio finanziario	Interno	1 - 4	5	2	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Lista controllo accessi (ACL) cartelle archivio
Documenti informatici archivio servizio personale associato	Interno	1 - 2 - 4 - 9 - 10	1 - 5 - 8 - 9	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Lista controllo accessi (ACL) cartelle archivio
Software gestione rilevazione presenze e gestione personale	Interno	1 - 4 - 9 - 10	8 - 9	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Accesso all'applicativo tramite assegnazione di profili e permessi
Software gestione paghe	Esterno	1 - 4 - 9 - 10	8 - 9	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Accesso all'applicativo tramite assegnazione di profili e permessi
Documenti informatici archivio servizio politiche	Interno	1 - 2 - 4 - 6 - 8 - 10	1 - 3 - 5 - 8 - 9	3	Sistema di autenticazione di accesso dell'utente alla rete telematica

educative					Lista controllo accessi (ACL) cartelle archivio
Software gestione sportelli sociali, cartella sociale e valutazione multidimensionale	Interno	1 - 4 - 5 - 6 - 8 - 10	1 - 8	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Accesso all'applicativo tramite assegnazione di profili e permessi
Software gestione autorizzazioni interventi servizio sociale integrato	Interno	1 - 4 - 5 - 6 - 8 - 10	1 - 8	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Accesso all'applicativo tramite assegnazione di profili e permessi
Documenti informatici archivio Servizio Sociale Integrato	Interno	1 - 4 - 5 - 6 - 8 - 10	1 - 8	6	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Lista controllo accessi (ACL) cartelle archivio
Piattaforme degli enti erogatori dei benefici	Esterno	1 - 4 - 6	1 - 8	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Accesso alla piattaforma tramite user e password
Documenti informatici archivio Servizi Sociali Territoriali	Esterno	1 - 4 - 5 - 6 - 8 - 10	1 - 8	6	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Lista controllo accessi (ACL) cartelle archivio
Software gestione riscossione coattiva	Interno	1 - 10	1 - 4	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Accesso all'applicativo tramite assegnazione di profili e permessi
Software gestione procedure relative al codice della strada	Interno	1 - 4 -10	Tutti i cittadini	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Accesso all'applicativo tramite assegnazione di profili e permessi
Software gestione infortunistica stradale	Interno	1 - 4 -10	Tutti i Cittadini	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Accesso all'applicativo tramite assegnazione di profili e permessi
Documenti informatici archivio polizia municipale	Interno	1 - 4	Tutti i Cittadini	3	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Lista controllo accessi (ACL) cartelle archivio

Videosorveglianza	Interne ed esterna	1 - 10	Tutti i Cittadini	6	Sistema di autenticazione di accesso dell'utente alla rete telematica
					Accesso al sistema tramite user e password
Sistema di posta elettronica	Interno	1 - 4 - 6 - 8 - 10	1 - 3 - 5 - 8	3	Accesso al sistema tramite user e password

2.5 Analisi dei depositi fisici di dati personali

Sempre partendo dell'analisi per processo svolta con il Registro e il DPIA, si riaggregano i dati personali per deposito fisico (es. stanza, archivio, armadio, cassaforte) valutando, in analogia a quanto già effettuato per i processi, i rischi ai dati personali derivanti da un accesso non autorizzato a questi depositi o dalla loro distruzione:

DEPOSITO	INTERNO/ ESTERNO	CONTROLLO ACCESSI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI SOGGETTI INTERESSATI	PROBABILITA' VIOLAZIONE	IMPATTO VIOLAZIONE	INDICE DI RISCHIO	NOTE: MISURE DI SICUREZZA ORGANIZZATIVE IN ATTO
Archivio Ufficio Appalti	INTERNI	SI	1 10	5 7	1	3	3	Ufficio chiuso a chiave
Archivio Segreteria	INTERNI	SI	Tutti	Tutti	1	3	3	Armadio riservato all'ufficio, in ufficio chiuso a chiave
Archivio Servizi Finanziari	INTERNI	SI	1 4	5	1	2	2	Armadio riservato all'ufficio, in ufficio chiuso a chiave
Archivio ufficio Risorse Umane	INTERNI	SI	1 2 4 9 10	1 5 8 9	1	3	3	Armadio chiuso a chiave contenente fascicoli cartacei delle procedure concorsuali, con domande e documentazione relativa ai partecipanti, e fascicoli cartacei dei dipendenti
Archivio ufficio Politiche Educative	INTERNI	SI	1-2-4-6-8-10	1-3-5(insegnanti di altre scuole)-8-9 (insegnanti dipendenti dei Comuni)	1	3	3	Armadio dotato di serratura con documentazione cartacea di lavoro
Archivio ufficio amministrativo SSI	INTERNI	SI	1-4-5-6-8-10	1-8	1	3	3	Armadio blindato/chiuso a chiave Schedari chiusi a chiave in ufficio chiuso a chiave durante l'assenza del personale
Archivio ufficio Minori SSI	INTERNI	SI	1-4-5-6-8-10	1-8	1	3	3	Schedari chiusi a chiave in ufficio chiuso a chiave durante l'assenza del personale
Archivio ufficio disabili SSI	INTERNI	SI	1-4-5-6-8-10		1	2	2	Armadio blindato e armadi d'ufficio chiusi a chiave in ufficio chiuso a chiave durante l'assenza del personale
Archivio ufficio "Centro Famiglie" SSI	INTERNI	SI	1-4-5-6-8-10	1-8	1	2	2	Schedari chiusi a chiave in ufficio chiuso a chiave durante l'assenza del personale
Archivio Ufficio SST Bibbiano	INTERNI	SI	1-4 -5-6-8-10	1 - 8	1	2	2	Armadio blindato/chiuso a chiave in ufficio chiuso a chiave durante l'assenza del personale

Archivio Ufficio SST Canossa	INTERNI	SI	1-4 -5-6-8-10	1 - 8	1	2	2	Armadio blindato/chiuso a chiave in ufficio chiuso a chiave durante l'assenza del personale
Archivio Ufficio SST San Polo d'Enza	INTERNI	SI	1-4 -5-6-8-10	1 - 8	1	2	2	Armadio blindato/chiuso a chiave in ufficio chiuso a chiave durante l'assenza del personale
Archivio Ufficio SST Montecchio E.	INTERNI	SI	1-4 -5-6-8-10	1 - 8	1	2	2	Armadio blindato/chiuso a chiave in ufficio chiuso a chiave durante l'assenza del personale
Archivio Ufficio SST Cavriago	INTERNI	SI	1-4 -5-6-8-10	1 - 8	1	2	2	Armadio blindato/chiuso a chiave in ufficio chiuso a chiave durante l'assenza del personale
Archivio Ufficio SST Sant'Ilario d'Enza	INTERNI	SI	1-4 -5-6-8-10	1 - 8	1	2	2	Armadio chiuso a chiave (per conservare documenti con dati giudiziari) in ufficio chiuso a chiave durente l'assenza del personale
Archivio Ufficio SST Campegine	INTERNI	SI	1-4 -5-6-8-10	1-8	2	2	4	Armadio chiuso a chiave
Archivio Ufficio SST Gattatico	INTERNI	SI	1-4 -5-6-8-10	1 - 8	1	2	2	Armadio chiuso a chiave in ufficio chiuso e allarmato durante l'assenza del personale
Archivio ufficio riscossione coattiva (Gattatico)	INTERNI	SI	1-10	1-4	1	2	2	Ufficio chiuso a chiave durante l'assenza del personale e armadi chiusi a chiave
Archivio centrale operativa PM	INTERNI	SI	1-3-4-5-6-7-8-10	Tutti i Cittadini	1	3	3	Armadio chiuso a chiave in cui sono tenuti i fascicoli e chiave in armadio blindato. Accessi in centrale operativa controllati e riservati.

2.6 Predisposizione di sistemi di monitoraggio e di valutazione delle vulnerabilità

Con riferimento all'analisi svolta in ottemperanza ad AGDI2/2017, si elencano i sistemi di monitoraggio (es. Intrusion Detection System, antivirus) e di valutazione delle vulnerabilità (es. penetration test, scanner di porte di rete) già operativi nell'Ente:

SISTEMA	INTERNO / ESTERNO	TIPOLOGIA	CHI AVVISA / LO UTILIZZA NEL TEAM	ALTRE INFORMAZINI
Antivirus	Interno	F-Secure Antivirus	Amministratore di sistema	
Firewall con advanced content security software	Interno	Endian Virtual	Amministratore di sistema	

2.7 Predisposizione del sistema di segnalazione

Oltre agli eventuali alert dai sistemi di monitoraggio, le segnalazioni di potenziali data breach possono provenire da persone (interne ed esterne all'Ente), che devono quindi disporre di un sistema di inoltro della segnalazione al team ed averne adeguata conoscenza.

Il sistema deve tenere traccia dell'avvenuta segnalazione e, possibilmente, essere collegato al sistema di registrazione dei data breach.

Il sistema deve prevedere meccanismi di backup / escalation tra le persone cui viene inoltrata la segnalazione.

Sistema	Rivolto a / Usato da	Pubblicizzato attraverso	Meccanismo di backup / escalation	Collegato al sistema di registrazione dei data breach
Posta elettronica	Cittadino	Sito istituzionale dell'Ente, nella informativa sul trattamento dei dati.	Modulo word stampato	No

2.8 Predisposizione del sistema di registrazione (Registro data breach)

L'art. 35 comma 5 del GDPR specifica che la documentazione relativa ai data breach consente all'Autorità di verificare il rispetto delle prescrizioni.

Poiché il GDPR e le DBGL prevedono casi in cui tale documentazione sia trasmessa all'Autorità a distanza di tempo dall'accadimento dell'evento (es. un data breach non notificato sul momento che riveli solo in un secondo tempo la sua pericolosità) appare raccomandabile, come previsto da ISO27035, che l'Ente si doti di un sistema informativo di registrazione dei data breach, notificati o meno all'Autorità.

Le DBGL evidenziano che il GDPR non specifica per quanto tempo occorra conservare la documentazione relativa ai data breach e che essa può, a sua volta, contenere dati personali e quindi rientrare nel Registro delle attività di trattamento e nel DPIA.

Poiché il sistema di registrazione dei data breach potrebbe risultare non disponibile durante un evento che coinvolga l'infrastruttura informatica, è opporuno prevedere un sistema di backup per la produzione e la trasmissione del report da inviare all'Autorità.

Sistema	**Interno / Esterno**	**Descritto nel Registro di trattamento dei dati**	**Analizzato nel DPIA**	**Altre informazioni**
Sistema principale MANTIS	Interno	No	No	Sistema di ticketing interno
Sistema di backup: back del sistema Mantis e modulo excel stampato	Interno	No	No	

3 Attività di esecuzione

3.1 Flusso generale

Il flusso generale di esecuzione delle attività in caso di (potenziale) data breach è il seguente:

- Segnalazione del potenziale data breach
- Valutazione della segnalazione
    - Se è un data breach, valutazione del rischio:
        - Se è "probabile" o "elevato", notifica all'Autorità (in copia anche al DPO)
        - Se è "elevato" e la situazione lo consente, comunicazione agli Interessati
        - Risposta al data breach
- Registrazione delle valutazioni e delle azioni eseguite

3.2 Segnalazione del potenziale data breach

Le attività di gestione di un (potenziale) data breach sono eseguite a partire da:

- una segnalazione automatica proveniente dai sistemi di monitoraggio ed alert
- una segnalazione inoltrata da una persona - interno o esterna all'Ente – attraverso il sistema di segnalazione predisposto allo scopo

Entrambe le vie garantiscono la registrazione dell'avvenuta segnalazione ai fini di documentare la successiva presa in carico.

La segnalazione può essere endogena al team.

In questa fase non è vi è ancora evidenza che si sia intercettato un vero e proprio data breach e quindi non scattano ancora le 72 ore concesse dal GDPR per la notifica all'Autorità.

3.3 Valutazione della segnalazione

Questa attività ha lo scopo di evitare le attività successive in caso di falso positivo (es. temporaneo malfunzionamento della connessione o del sistema di monitoraggio, segnalazione manifestatamente infondata ecc.). Il riferimento per la valutazione è la definizione contenuta nell'art.4 comma 12 del GDPR

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Per le DBGL, si è in presenza di un data breach se è accertata almeno una delle seguenti violazioni:

- violazione della confidenzialità (confidentiality breach)
- violazione della disponibilità (availability breach)
- violazione della integrità (integrity breach)

Per l'esecuzione della valutazione, si utilizza la procedura operativa predisposta allo scopo.

La valutazione è svolta da	Il Responsabile (di settore)
che registra l'esito della valutazione	nel Registro dei Data Breach
In caso di valutazione negativa	Il Responsabile chiude la segnalazione nel Registro. Il Delegato analizza trimestralmente il Registro.
In caso di valutazione positiva	Il Responsabile avvisa il Delegato sottoponendo il data breach alla sua validazione, registrando il passaggio nel Registro di Data Breach

Questo flusso della valutazione della segnalazione ottempera l'art.33 comma 2 del GDPR.

Poiché è responsabilità del Delegato stabilire se in via definitiva se l'ipotesi di data breach avanzata dal Responsabile di Settore, le 72 ore non partono dalla comunicazione del Responsabile di Settore verso il Delegato, ma solo al termine della successiva verifica da parte del Delegato. In questo senso si interpreta la "conoscenza" dell'Art. 22 comma 1:

Art.33(1) GDPR "*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità … senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*"

3.4 Valutazione del rischio

Se si è di fronte ad un data breach, il Delegato provvede alla valutazione del rischio, classificando il caso secondo i tre livelli descritti dagli artt. 33 e 34 del GDPR:

Livello	Valutazione	Notifica alla	Comunicazione

		Autorità	agli Interessati
Rischio improbabile	È improbabile che vi sia un rischio per i diritti e le libertà della persona fisica dell'Interessato Art. 33(1)	No	No
Rischio probabile	E' probabile che vi sia un rischio per i diritti e le libertà della persona fisica dell'Interessato Art.33(1)	Si	No
Rischio elevato	E' suscettibile di presentare un rischio elevato per i diritti e le libertà dell'Interessato Art.34(1)	Si	Dipende

La valutazione del rischio definisce quindi la necessità o meno di procedere alle attività successive (escluse quelle di registrazione, comunque obbligatorie).

Rispetto alla valutazione effettuata in sede di DPIA, la valutazione di data breach persegue uno scopo più mirato: se nel DPIA si valutano conseguenze potenziali nel caso si verifichi un'ipotetica violazione, nel caso di data breach occorre ricalibrare la valutazione effettuata nel DPIA considerando le concrete circostanze della violazione.

L'esito della valutazione del rischio è registrata nel Registro dei data breach, corredata da una sintetica motivazione.

3.5 Notifica all'Autorità di Controllo

La notifica all'Autorità di Controllo è compito assegnato dall'Art. 33 del GDPR al Titolare che provvede, direttamente o attraverso il Delegato, a trasmettere la notifica dall'Autorità di Controllo, assumendosene comunque la responsabilità.

Potendosi trovare il Titolare o Delegato a dover decidere in un contesto di informazioni incomplete, il GDPR mette a disposizione alcune modalità che tendono a contemperare le esigenze – potenzialmente contrastanti – di celerità e di accuratezza nella notifica all'Autorità:

notifica approssimata	Se non è noto con certezza il numero delle persone e dei dati personali coinvolti nel data breach, in prima battuta il titolare può notificare all'Autorità una stima approssimativa provvedendo, in seguito ad accertamenti più puntuali, a comunicare dati più accurati.
notifica per fasi	In situazioni complesse, il titolare può notificare subito un sintetico alert, aggiornando l'Autorità per fasi successive sulla base di nuovi riscontri.
notifica aggregata	In caso di violazioni ripetute e simili, per ridurre l'aggravio di continue notifiche il titolare può eseguire una notifica aggregata di tutte le violazioni subite in un arco di tempo anche superiore alle 72

	ore, giustificando nella notifica le motivazioni del ritardo.

In assenza di diverse istruzioni da parte dell'Autorità e disponendo dei mezzi informatici necessari, il Titolare trasmette la notifica all'Autorità via PEC utilizzando il modulo predisposto dall'Autorità o, se risultasse più semplice e veloce, attraverso un documento diversamente formattato ma di eguale contenuto.

Non disponendo dei mezzi informatici necessari, il Titolare provvede alla trasmissione della notifica all'Autorità attraverso altro mezzo di comunicazione (mail normale, telefono) provvedendo in un secondo tempo alla ritrasmissione via PEC.

L'avvenuta notifica viene registrata nel Registro dei Data Breach specificando contenuti, tempi e modalità e, se il caso, se si è utilizzata una delle modalità sopra ricordate.

3.6 Comunicazione agli Interessati

La comunicazione agli Interessati è compito assegnato dall'Art. 33 del GDPR al Titolare che vi provvede, direttamente o attraverso un Delegato allo scopo.

Anche se si è nel caso di "rischio elevato", l'Art.34 comma 3 del GDPR esclude l'obbligo di comunicazione in alcuni casi:

"Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) *il titolare ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;*
b) *il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;*
c) *detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia."*

Il caso b) consente al Titolare di soprassedere alla comunicazione agli interessati qualora la risposta messa in campo in contrasto al data breach sia valutata adeguata ad riportare il rischio a livello "probabile" o "nullo".

Il comma successivo e i Considerando n.86 e n.88 coinvolgono l'Autorità nel processo decisionale che porta o meno alla comunicazione:

Art. 34(4): *"Nel caso in cui il titolare non abbia ancora comunicato all'interessato la violazione, l'Autorità può richiedere, dopo aver valutato la probabilità che la violazione presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta."*

C86 "*Le comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'Autorità e nel rispetto degli orientamenti impartiti da questa... Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.*"

C88 "Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali."

La comunicazione agli interessati richiede la disponibilità non solo dell'elenco dei nominativi degli interessati, ma anche la conoscenza di un loro recapito certo (es. indirizzo email). Nella comunicazione deve essere utilizzato un linguaggio semplice e comprensibile dagli interessati.

Nel caso di comunicazione pubblica previsto dall'Art. 34 comma 3d, deve essere garantita la medesima efficacia conoscitiva che si sarebbe ottenuta con una comunicazione diretta all'interessato, ponendo ad esempio la comunicazione in adeguata evidenza sul sito internet dell'Ente.

Diversamente dal caso della notifica all'Autorità, il GDPR non specifica il contenuto della comunicazione, che dovrà tenere conto delle cautele espresse dal C86 e C88.

Nel Registro dei data breach viene annotato l'esito della valutazione sulla necessità / inopportunità / impossibilità di procedere alla comunicazione e, in caso positivo, la sintesi delle modalità scelte per la comunicazione allegando, quando tecnicamente possibile, l'elenco degli interessati o almeno una indicazione della categoria degli interessati, in analogia a quanto richiesto dalla notifica all'Autorità.

3.7 Informativa al DPO

Poiché l'Autorità di Controllo può richiedere la collaborazione del DPO (*Data Protection Officer*) nella valutazione della situazione, come raccomandato dalle DBGL è opportuno che il DPO venga avvisato dell'avvenuta violazione dei dati personali, inviando al suo recapito copia della notifica inviata all'Autorità.

3.8 Azioni di risposta al data breach

Come accennato nell'Art.34 comma 3c del GDPR ("*il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati")* la tempestiva esecuzione di azioni di risposta al data breach può significativamente

incidere positivamente sull'esito finale della gestione del caso, evitando ad esempio la comunicazione agli interessati ed i conseguenti effetti negativi (sia finanziari sia di immagine) sull'Ente.

Le risposte devono basarsi per quanto applicabile sulle procedure operative predisposte allo scopo o su altre pratiche consolidate dall'uso.

3.9 Registrazione delle valutazioni e delle azioni

Al termine della gestione del data breach, il Registro dovrà contenere tutte le informazioni relative al caso, incluse le decisioni assunte e le azioni messe in campo, secondo lo schema riportato al termine del presente documento.

4 Attività di miglioramento

Le attività di miglioramento hanno l'obiettivo di mettere a punto un elenco di migliorie apportabili alla gestione dei data breach relative a tutte le fasi del ciclo, partendo dalla analisi dei casi di data breach registrati nel Registro.

Il Registro dei data breach assume quindi il duplice scopo di consentire di rispondere adeguatamente all'Autorità di Controllo e di fornire gli elementi base per il miglioramento continuo del sistema, desumendo dall'osservazione collettiva dei casi occorsi alcune "lezioni imparate" dai precedenti fallimenti e successi.

Dall'analisi del Registro si possono trarre alcuni indicatori, utili sia per identificare aree di debolezza nel sistema di protezione dei dati personali sia, col passare degli anni, per valutare la stabilità del sistema e la sua adeguatezza a resistere a nuove minacce (tra parentesi, il valore ideale obiettivo):

- Numero di data breach per anno e per settore organizzativo dell'Ente (0)
- Numero di notifiche (come sopra) (0)
- Numero di notifiche differite / per fasi (come sopra) (0)
- Numero di comunicazioni (come sopra) (0)
- Numero segnalazioni dall'esterno / totale segnalazioni (0)
- Numero segnalazioni automatiche / totale segnalazioni (1)
- Numero data breach assistiti da procedura operativa / totale data breach (1)
- Tempo medio trascorso tra evento e la sua "conoscenza" (0)

5 Schema per il Registro dei data breach

Fase	Informazione	Nota
Segnalazione	Data e ora segnalazione	
	Segnalatore	interna / esterna, personale / automatica
	Contenuto della segnalazione	
Valutazione segnalazione	Data e ora avvio valutazione	
	Incaricato o Resp. della valutazione	
	Sintesi segnalazione	
	Procedure applicate	
	Controlli extra procedure eseguiti	
	Esito valutazione	
	Sintesi motivazioni della valutazione	
Se la valutazione è positiva	Data ed ora inizio evento	Può essere presunta
	Data ed ora fine evento	Può anche essere presunta o ancora in corso
	Tipi violazioni accertata	Confidenzialità / disponibilità / integrità
	Sistemi informativi / database coinvolti	
	Procedimenti coinvolti	
	Unità organizzative coinvolte	
	Categorie di interessati	
	Quantità di interessati	
	Categorie di dati personali	
	Trattamenti eseguiti dalla violazione	
	Altri coinvolti nella valutazione	Soprattutto se responsabili esterni
	Data e ora di conclusione della valutazione	Le 72 ore partono da qui
Valutazione del rischio	Data e ora avvio valutazione	
	Titolare o Resp. della valutazione	
	Altri coinvolti nella valutazione	Soprattutto se resp. esterni
	Valutazione del livello di rischio	
	Sintesi motivazioni del livello	
Notifica (livello “probabile” o “elevato”)	Data e ora avvio notifica	Qui si concludono le 72 ore
	Titolare / delegato della notifica	
	Copia della notifica	
	Copia allegati alla notifica	
	Modalità di inoltro della notifica	
	Note relative notifiche successive	
	Data e ora fine notifiche	
Comunicazione (livello	Data e ora avvio comunicazioni	
	Responsabile / Incaricato che esegue la	

“elevato”)	comunicazione	
	Esito valutazione necessità di comunicare	
	Motivazioni per mancata comunicazione	
	Modalità coinvolgimento Autorità	
	Quantità interessati cui comunicare	
	Modalità di comunicazione	
	Contenuto della comunicazione	
	Data e ora fine comunicazioni	
Avviso a DPO	Data e ora avviso DPO	
	Incaricato dell’avviso	
	Modalità e contenuto avviso	
Risposta	Data e ora inizio azioni di risposta	
	Inseritore che registra le azioni	
	Procedure applicate	
	Azioni extra procedure eseguite	
	Valutazione esito risposte sul rischio	
	Data e ora fine azioni	