Regolamento per il monitoraggio e la gestione delle violazioni di dati (data breach)

Stazione Zoologica "Anton Dohrn"
Istituto Nazionale di Biologia, Ecologia e Biotecnologie Marine

(Approvato con delibera del Consiglio di Amministrazione n. 28 del 12/03/2020)

Stazione Zoologica Anton Dohrn Napoli

Procedura per il monitoraggio e la gestione delle violazioni di dati (*data breach*)

Art. 1 - Scopo

La presente procedura ha lo scopo di descrivere le attività che la Stazione Zoologica di Napoli deve porre in essere per gestire gli incidenti e le violazioni dei dati personali ai sensi degli artt. 33-34 del Regolamento (UE) 2016/679.La presente procedura di Data Breach è disponile nella Intranet aziendale della Stazione, in modo da favorirne la consultazione da parte di tutti i destinatari.

La mail di contatto per le segnalazioni è privacy@szn.it e ogni segnalazione verrà reindirizzata nella casella di posta elettronica del *Data Protection Officer* (DPO), del Direttore Generale e del Legale rappresentante (Presidente).

Art. 2 - Ruoli e Responsabilità

Tutto il personale aziendale è responsabile per la SEGNALAZIONE di eventuali Data Breach. Per la GESTIONE della crisi conseguente ad un evento di Data Breach è necessario costituire un Data Breach Management Team (di seguito, il "Team"), chiamato a svolgere una funzione di guida in merito alle modalità operative che tutta l'organizzazione dovrà adottare e con particolare riferimento all'attività di comunicazione.

Il team è composto dalle seguenti figure:

- Direttore delegato dal Titolare del trattamento (i.e., il Presidente quale Rappresentate Legale);
- DPO che funge anche da interfaccia con il Garante;
- Privacy Manager (PRG e/o PRI, per il riscontro al Garante o all'Interessato); in assenza di specifica designazione del Privacy Manager, questi coincide con il Delegato per la protezione dei dati.
- Un riferimento per ciascuna area aziendale:
- Altre funzioni saranno coinvolte in base all'evento (Responsabili esterni, ecc.).

Art.3 - Ambito di applicazione

Per Data Breach (o "Violazione dei dati personali") si intende un incidente di sicurezza, per effetto del quale, non si è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali, 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 (Art. 4 p.12 GDPR).

L'obbligo di notifica all'Autorità si impone se la violazione comporta, ragionevolmente, un rischio per i diritti e le libertà delle persone fisiche; qualora, poi, il rischio fosse elevato, o se richiesto o disposto dall'Autorità, il titolare sarà tenuto a darne comunicazione all'interessato.

I principali rischi sono i seguenti:

- perdita del controllo dei dati degli interessati;
- limitazioni dei diritti/discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie/danno economico o sociale o reputazionale (sia per l'interessato che per il Titolare);
- decifratura non autorizzata della eventuale pseudonimizzazione applicata ai dati;
- perdita di riservatezza dei dati personali di particolari ("sensibili").

Si possono distinguere tre tipi di violazioni, che potrebbero essere combinate tra loro:

1) Violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.

2) Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.

3) Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Sono dunque monitorati e considerati i seguenti eventi:
• distruzione, perdita, alterazione, anche accidentali,
• archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti.

Solitamente il Data Breach si realizza con una divulgazione di dati personali all'interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria, ad esempio, quando i dati personali sono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

Tale divulgazione potrebbe avvenire, ad esempio in seguito a:

i) perdita accidentale: ad esempio, Data Breach causato da smarrimento di una chiavetta USB contenente dati riservati;
ii) furto: ad esempio, Data Breach causato da furto di un notebook contenente dati confidenziali;
iii) infedeltà aziendale: ad esempio, Data Breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico;
iv) *accesso abusivo: ad esempio, Data Breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite.*

Art. 4 - Verifica di efficacia della procedura e modalità operative

L'efficacia della presente procedura verrà valutata mediante audit semestrale volto a verificare la correttezza dello svolgimento della procedura. Tutte le attività e le riunioni del *Team* devono essere documentate ed i verbali sono conservati dal Responsabile del *Team*.

Almeno una volta all'anno, il DPO predispone una relazione sulla attività del *Team* nel corso dell'anno. Tale relazione viene trasmessa al Rappresentante Legale ed al Direttore Generale.

La relazione dovrà, per quanto possibile, essere integrata da dati numerici per comprendere l'entità degli eventi ed i tempi di reazione.

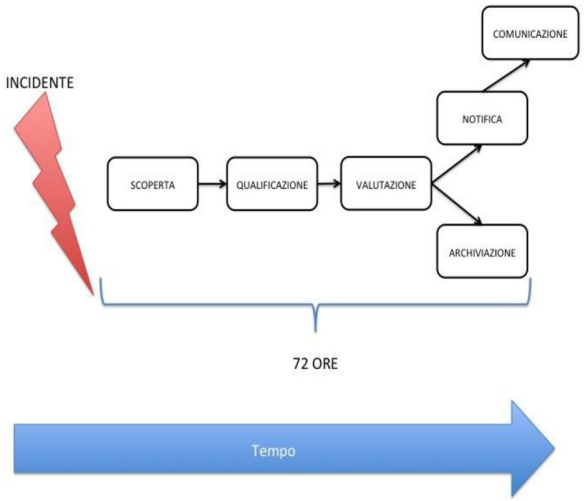
Art. 5 - Criteri applicabili

Le segnalazioni circa gli incidenti che potrebbero sfociare in un Data Breach:

1) Sono fatte dagli autorizzati e responsabili al Privacy Manager;
2) Sono fatte dagli interessati e da terzi al punto di contatto privacy presidiato;
3) Derivano dai sistemi di monitoraggio automatici dei sistemi informatici (in quanto la responsabilità è anche commisurata secondo la capacità di scoprire tempestivamente un incidente ed indagarlo).

Ricevuta la segnalazione, il Privacy Manager coinvolge il DPO, e il Delegato alla protezione dei dati; deve identificare l'incidente di sicurezza, comprendere se l'incidente ha impatto sulle informazioni e, infine, determinare se tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'obbligo di notificazione al Garante (entro 72 ore dalla scoperta) e quello aggiuntivo di comunicazione agli interessati coinvolti devono essere valutati caso per caso in relazione ai diritti ed alla libertà degli interessati e tenuto conto che, in particolare per tale seconda comunicazione non è dovuta se il rischio per gli interessati non elevato o se si utilizzano (e lo si può dimostrare) misure, come ad esempio la cifratura, che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate al momento della violazione.



Le attività di scoperta dell'incidente e quelle successive di gestione sono documentate adeguatamente (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

Ogni violazione dei dati personali è annotata nel **Registro delle Violazioni dei Dati** (acronimo **RVD**) e contiene

- la data in cui è annotata,
- la data della sua scoperta,
- le circostanze a essa relative,
- la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- le conseguenze ipotizzate all'atto della scoperta,
- le misure e i provvedimenti adottati e da adottare per porvi rimedio e anche, se del caso, per attenuarne i possibili effetti negativi, indicando tempistiche e soggetti preposti al loro assolvimento,
- la valutazione dei rischi per i diritti e le libertà delle persone fisiche relativamente alla violazione in questione, con l'indicazione della necessità o meno di provvedere alla notificazione ai sensi dell'art. 33 del GDPR all'Autorità di controllo e/o alle comunicazioni ai sensi dell'art. 34 del GDPR agli interessati,
- il riferimento alla notificazione ai sensi dell'art. 33 del GDPR all'Autorità di controllo, gestita secondo le corrette modalità di comunicazione, dettagliando anche il momento e il mezzo del suo invio,
- il riferimento alle comunicazioni ai sensi dell'art. 34 del GDPR agli interessati, gestita secondo le corrette modalità di comunicazione, dettagliando anche il momento e il mezzo del suo invio,
- uno o più riesami con l'indicazione dell'evoluzione delle conseguenze della violazione fino alla sua chiusura; i riesami contengono la data in cui esso avviene, le conseguenze realizzatesi a causa della violazione, la valutazione circa i provvedimenti adottati, l'aggiornamento delle indicazioni in merito ai provvedimenti da adottare.

Art. 6 - Descrizione processo e definizione dei compiti

Qualora il personale interno (lavoratori, collaboratori, autorizzati, preposti, responsabili, ecc.) dovesse rilevare che si è verificato un Data Breach ovvero che vi è un rischio serio ed imminente di violazione dei dati personali detenuti, dovrà seguire la **procedura** di seguito descritta, con la massima puntualità ed efficienza.

Scoperta: La scoperta di un incidente di sicurezza può essere svolta da diversi attori

1) dagli autorizzati e responsabili al Privacy Manager;
2) dai sistemi di monitoraggio automatici dei sistemi informatici;
3) dagli interessati e da terzi al punto di contatto privacy presidiato.

Esempi

- Violazioni del sistema informatico
- Hackeraggio
- Perdita di dispositivi aziendali
- Attivazione di Cryptolocker
- Accesso non autorizzato ad archivi cartacei.

Nei primi due casi è opportuno che l'attore attivi una pronta risposta per contrastare la minaccia che dipende da caso a caso.

Esempio - nel caso di incidente informatico legato a malware: • scollegare il terminale dalla rete ethernet e/o disattivare Wi-Fi • attivare il software antivirus e far eseguire un ciclo di analisi

In ogni caso il soggetto interno che prende coscienza dell'incidente di sicurezza, informa tempestivamente il Privacy Manager e il DPO, ove designato, che procede/procedono alla fase successiva di qualificazione dell'incidente.

Qualificazione dell'incidente

Se l'incidente di sicurezza ha impatto (a qualunque livello) su informazioni (documenti, file, strumenti, servizi, ecc.) contenenti dati personali allora si tratta di una violazione di dati e va valutata (fase di valutazione dell'impatto della violazione) per determinare tipologia e quantità dei dati personali oggetto del data breach e individuare contromisure tecniche correttive e preventive; altrimenti l'incidente non deve essere preso in considerazione ai fini della presente procedura.

Ogni violazione dei dati personali è dunque annotata (art. 33 p.5 GDPR) **nel Registro delle Violazioni dei Dati (RVD),** come specificato sopra.

Le annotazioni nel RVD garantiscono che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notificazione, il cui scopo è di limitare i danni che possono derivare per effetto di una violazione a carico degli interessati, fatto che dipende dalla tempestività e dall'adeguatezza con cui la violazione è affrontata. La comunicazione invece risponde allo scopo di consentire all'interessato, qualora sussista una violazione che presenta rischi elevati, di prendere le precauzioni necessarie.

Contenimento e adozione di contromisure

Contestualmente alla qualificazione occorre continuare a perseguire le misure per bloccare e contenere le conseguenze dannose dell'incidente, iniziate nella fase di scoperta, coinvolgendo altri soggetti (es. preposto ICT, amministratori di sistema, ecc.).

Valutazione dell'impatto della violazione

Nel determinare l'obbligo di notificazione e di successiva comunicazione occorre valutare la possibilità che la violazione possa causare danni fisici, materiali o immateriali alla persona fisica, quali ad esempio (Considerando 85 GDPR):

- perdita del controllo dei dati personali degli interessati;
- limitazione dei 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, o qualsiasi altro danno economico o sociale significativo per la persona interessata.

Nel dettaglio si applica la metodologia sviluppata dall'ENISA (European Union Agency for Network and Information Security) pubblicata nel dicembre 2013, riportata di seguito nelle parti fondamentali all'art. 10, per definire se il Data Breach verificatosi possa comportare un rischio per i diritti e le libertà delle persone fisiche i cui dati personali sono stati violati e se, conseguentemente se debbano essere fatte le comunicazioni di cui agli Artt. 33 e/o 34 del GDPR al Garante ed agli interessati.

Per tale valutazione sono utilizzate le informazioni riportate in fase di scoperta, di contenimento e adozione delle contromisure. Se necessario, si consultano i legali per acquisire un parere in proposito.

Aspetti decisionali

Il Titolare del trattamento deve essere sempre informato degli sviluppi e delle decisioni del Team in ogni fase dell'indagine ed ha potere di imporre misure più restrittive a tutela dei diritti degli interessati. Qualora il Titolare non fosse disponibile a fornire il contributo richiesto; il Direttore Generale di concerto con il DPO ha l'autorità per procedere autonomamente nelle decisioni prese.

Qualora non condividesse la decisione presa dal Team e la valutasse eccessiva in quanto ritiene possa impattare negativamente sulla reputazione/immagine della Stazione o ledere gli interessi economici della stessa, il Titolare si assume la responsabilità di imporre la sua decisione.

In questo caso, il Team verbalizzerà la decisione del Titolare nel Modulo Gestione del Data Breach sezione - Decisione di interruzione dell'analisi da parte del Titolare, nonché la posizione del Team ed archivierà la documentazione senza procedere ulteriormente, tramite comunicazioni con data certa (es. tramite PEC) al Titolare.

In ogni caso, il DPO è autonomo nel valutare, in caso di contrasto con il Titolare del Trattamento, se comunicare l'evento occorso direttamente al Garante nelle forme e modi che ritiene opportuni.

All'occorrenza, possono essere coinvolti esperti esterni che saranno incaricati della valutazione dell'evento previa sottoscrizione di un vincolo di riservatezza.

Art. 7 - Trattamento svolto come responsabile

Quando il trattamento oggetto della violazione è svolto in qualità di responsabile o sub-responsabile per conto del Titolare del trattamento, a cui spetta l'obbligo di notificazione a meno di diverse pattuizioni contrattuali, vige il dovere di informare tale Titolare senza ingiustificato ritardo quando si viene a conoscenza di una violazione e di supportarlo nel valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati.

Art. 8 - Trattamento svolto come titolare

a. Se NON SUSSISTE il rischio per i diritti e le libertà delle persone fisiche i cui dati personali sono stati violati

Si redige decisione scritta e motivata in merito alla valutazione di assenza di rischio e di non effettuare le comunicazioni di cui agli Artt. 33 e/o 34 del GDPR al Garante ed agli interessati, annotandola nel RVD. Allega alla stessa tutti i documenti, pareri, rapporti acquisiti.

b. Se SUSSISTE il rischio per i diritti e le libertà delle persone fisiche i cui dati personali sono stati violati Si procede alla notificazione (art.33 del GDPR) al Garante mediante PEC all'indirizzo (sulla base del formulario NG, vedi sotto):

protocollo@pec.gpdp.it

Se il rischio **è ELEVATO**, si procede alla comunicazione anche agli interessati (art.34 del GDPR), via e-mail, sms o a mezzo posta sulla base del formulario CI

Art. 9 Azioni a seguito delle decisioni

Sulla base della casistica in cui si ricade, debbono essere svolte le seguenti azioni:

caso A – basso rischio calcolato (livello di gravità della Violazione dati: basso)

- si aggiorna il modulo Gestione del Data Breach e si chiude l'evento senza eseguire ulteriori comunicazioni;

caso B - rischio che implica l'adozione di trattamento dell'evento ed eventuale Azione Correttiva (livello di gravità della Violazione dati: medio)

- si aggiorna il modulo Gestione del Data Breach e si procede con le eventuali Azioni Correttive comunicando internamente l'adozione delle azioni di trattamento convenute;

caso C - rischio che implica l'adozione di trattamento dell'evento, l'Azione Correttiva e la notifica obbligatoria all'Autorità di controllo

- si aggiorna il modulo Gestione del Data Breach ed il registro degli incidenti (M02 - Registro incidenti Data Breach);
- si procede con l'adozione di azioni di trattamento dell'evento con le Azioni Correttive;
- si procede con la notifica all'Autorità di controllo

caso D - rischio che implica, oltre a quanto previsto dal "caso C" anche la comunicazione obbligatoria agli interessati coinvolti

- si prepara un comunicato stampa da predisporre e verifica con DPO e Titolare del trattamento

Le notifiche all'autorità garante e le comunicazioni obbligatorie agli interessati devono avvenire massimo entro 8 ore dall'adozione della decisione.

Formulario NG (notificazione al Garante)

Modello di notifica al Garante per la protezione dei dati personali.
Da inviare a mezzo PEC all'indirizzo protocollo@pec.gpdp.it

Notifica di violazione dei dati personali (Data Breach) ai sensi dell'Art. 33 del RGPD

1. **Titolare del trattamento**

Denominazione o ragione sociale:
Provincia
Comune
Cap

Indirizzo:

Nome e cognome persona fisica addetta alla comunicazione

Indirizzo PEC e/o EMAIL per eventuali comunicazioni

Recapito telefonico per eventuali comunicazioni

2. Descrizione della violazione dei dati personali

….

3. Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

□ Il __/__/___

□ Tra il __/__/___e il __/__/___

In un tempo non ancora determinato

È possibile che sia ancora in corso

4. Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

5. Tipo di violazione

□ Lettura (presumibilmente i dati non sono stati copiati)
□ Copia (i dati sono ancora presenti sui sistemi del titolare)
□ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
□ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

□ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
□ Altro: …

6. Dispositivo oggetto della violazione
□ Computer
□ Rete
□ Dispositivo mobile
□ File o parte di un file
□ Strumento di backup
□ Documento cartaceo
□ Altro: …

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

…

8. Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?
□ N. persone
□ Circa persone
□ Un numero (ancora) sconosciuto di persone

9. Che tipo di dati sono oggetto di violazione?
□ Dati anagrafici/codice fiscale
□ Dati di accesso e di identificazione (user name, password, customer ID, altro)
□ Dati relativi a minori
□ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
□ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
□ Dati giudiziari
□ Copia per immagine su supporto informatico di documenti analogici
□ Ancora sconosciuto
□ Altro:

10. Livello di probabilità che della violazione dei dati personali possa comportare un rischio per i diritti e le libertà delle persone fisiche (secondo le valutazioni del titolare)?
□ Elevato
□ Medio
□ Basso
□ Trascurabile
□ Nullo

11. Misure tecniche e organizzative applicate ai dati oggetto di violazione

…

12. La violazione è stata comunicata anche agli interessati?
☐ Sì, è stata comunicata il
☐ No, perché ……..

13. Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Formulario CI (comunicazione all'interessato)

Oggetto: comunicazione ai sensi dell'Art. 34 del Regolamento Generale sulla Protezione dei Dati personali

Gentile Signora / Egregio Signore,
Siamo spiacenti di informarLa che, a causa di
☐ un problema tecnico dei nostri sistemi informatici
☐ un accesso non autorizzato alle nostre banche dati digitali / cartacee
☐ la perdita di un archivio digitale o cartaceo

si è verificata / potrebbe essersi verificata una violazione dei Suoi dati personali trattati dalla nostra azienda.

Per qualsiasi informazione in proposito, può rivolgersi al nostro servizio di assistenza scrivendo una e-mail all'indirizzo email privacy@szn.it.

Le probabili conseguenze della violazione dei Suoi dati personali potrebbero essere:

….

Al fine di porre rimedio alla violazione e per attenuarne i possibili effetti negativi, la nostra azienda ha adottato le seguenti misure:

….

Distinti saluti,

Art. 10 - Inintelligibilità dei dati

A giudizio dell'Autorità per Protezione dei Dati, si considerano inintelligibili i dati che, ad esempio:

a) siano stati cifrati in modo sicuro attraverso un algoritmo standardizzato, o mediante l´impiego di schemi di cifratura a chiave simmetrica o pubblica noti in letteratura, purché la chiave di decifrazione sia di adeguata lunghezza (espressa in numero di bit), sia stata predisposta dal titolare una policy per la relativa custodia, e se essa non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo da non consentirne la derivazione con gli strumenti tecnologici disponibili da parte di soggetti non autorizzati ad accedervi;

oppure

b) siano stati sostituiti da un valore di hash calcolato attraverso una funzione crittografica di hashing a chiave, purché la chiave utilizzata per effettuare lo hashing dei dati sia di adeguata lunghezza (espressa in numero di bit), sia stata predisposta dal titolare una policy per la relativa custodia, e se essa non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo da non consentirne la derivazione con gli strumenti tecnologici disponibili da parte di soggetti non autorizzati ad accedervi;

oppure

c) siano stati resi anonimi con procedure tali da non consentire la reidentificazione degli interessati cui si riferiscono da parte di soggetti non legittimati al loro trattamento, anche mediante il ricorso ad altre fonti informative disponibili presso il titolare o pubbliche.

Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) - 4 aprile 2013 (Pubblicato sulla Gazzetta Ufficiale n. 97 del 26 aprile 2013), Registro dei provvedimenti n. 161

Art. 11 - Metodologia di valutazione di impatto ENISA - dicembre 2013

INFORMAZIONI SULL'ENISA L'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) è un'agenzia dell'UE creata per promuovere il funzionamento del mercato interno. L'ENISA è un centro di eccellenza per gli Stati membri europei e le istituzioni europee in materia di sicurezza delle reti e delle informazioni, fornendo consigli e raccomandazioni e fungendo da centralino per le informazioni sulle buone pratiche. Inoltre, l'agenzia facilita i contatti tra le istituzioni europee, gli Stati membri e le imprese private e gli attori del settore. Questo lavoro si svolge nel contesto del programma ENISA per i rischi emergenti e futuri.

Internet: http://www.enisa.europa.eu/

Art. 12 - Registro delle Violazioni dei dati Il presente documento è istituito al fine di documentare e dare evidenza degli adempimenti in caso di violazione dei dati personali (artt. 5, 24, 33, 34)

Luogo, Data Firma

Data annotazione	Data scoperta	Circostanze e violazione	Conseguenze della violazione (ipotesi)	Natura della violazione	Misure e provvedimenti adottati	Valutazione dei rischi (artt. 33 e 34 del GDPR)	Riferimenti notificazione (art. 33 del GDPR)	Riferimenti comunicazione (art. 34 del GDPR)	Riesame delle Conseguenze (indicare la data del riesame

STAZIONE ZOOLOGICA ANTON DOHRN DI NAPOLI
Villa Comunale 80121 Napoli 081-5833218 stazione.zoologica@szn.it

Stazione Zoologica Anton Dohrn Napoli