ENTE NAZIONALE PER LA PROTEZIONE E L'ASSISTENZA DEI SORDI – ONLUS APS

Ente Morale che opera senza fini di lucro per l'integrazione dei sordi nella società

SEDE CENTRALE

CODICE DI CONDOTTA PER IL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 4 numero 7 del Reg. UE 2016/679 «il titolare del trattamento» è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Il Titolare del trattamento dati è ENS – Ente Nazionale per la protezione e l'assistenza dei Sordi ONLUS APS - con sede legale in Roma, Via Gregorio VII, n. 120, 00165 - Roma, legalmente rappresentato da Giuseppe PETRUCCI nato a Palma di Montechiaro (AG) il 05-01-1973 e domiciliato presso la sede sociale.
Ai sensi dell'art. 4 numero 8 del Reg. UE 2016/679 è «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.
Il responsabile del trattamento è nominato tra soggetti che per esperienza, capacità e affidabilità diano idonea garanzia del rispetto delle disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo della sicurezza. Tale figura presso l'ENS è ricoperta da Riccardo Avogadri (privacy@ens.it).
Presso ogni sede territoriale regionale e provinciale è stato individuato un sub responsabile del trattamento dei dati personali che è identificato con la figura apicale dell'ente stesso (Presidente o Commissario Straordinario Regionale e Provinciale).
Infine l'articolo 29 del Reg. UE. 2016/679 prescrive che chiunque agisca sotto l'autorità del Titolare del trattamento ovvero sotto quella del responsabile del trattamento e che abbia accesso a dati personali, non possa trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
Sono tre le tipologie di dati personali che possono essere trattati:

a) Art. 9 GDPR: Categorie Particolari: sono i dati personali idonei a rivelare "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
b) Art. 10 GDPR: Dati Personali relativi a condanne penali o reati;
c) Art. 4 n. 1 GDPR: «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

L'individuazione dei soggetti autorizzati può avvenire anche mediante la documentata preposizione di una persona fisica ad una unità per la quale è stato individuato l'ambito del trattamento consentito agli addetti all'unità medesima.
I trattamenti svolti in seno all'ENS possono essere di due specie:

a) trattamenti di primo livello, che riguardano attività trasversali e sono svolti utilizzando la rete e il sistema informativo automatizzato dell'Ente;
b) trattamenti di secondo livello: sono quelli specifici delle singole unità di trattamento, che sono monitorati e gestiti direttamente dai responsabili della Sede Territoriale, in qualità di responsabili del trattamento.

Si ricorda che ogni incaricato del trattamento, nel trattare i dati personali, deve rispettare i seguenti principi:

1) principio di finalità: il trattamento deve essere svolto per scopi determinati, espliciti e legittimi. Con riferimento all'Ente, questo limite è ancor più pregnante, considerato che l'Associazione è autorizzata al trattamento solamente se il trattamento è strumentale allo svolgimento di funzioni indicate nello statuto.
2) principio di proporzionalità: i dati, oggetto di trattamento, devono essere pertinenti, non eccedenti e completi rispetto agli scopi istituzionali perseguiti. La pertinenza attiene al merito dell'attività di trattamento; la non eccedenza alla quantità dei dati che possono essere raccolti e trattati in riferimento allo scopo perseguito; infine, la completezza attiene alla tutela dell'identità personale dell'interessato, che ha interesse a che il suo profilo e le informazioni detenute non siano parziali. Ove il trattamento riguardi categorie particolari di dati ovvero dati relativi a condanne penali o reati, occorre verificare caso per caso che i dati (di questa specie) siano indispensabili rispetto alla finalità perseguita;
3) principio di sicurezza: i dati oggetto di trattamento devono essere protetti attraverso l'adozione di misure di sicurezza.

Quale figura di garanzia, ai sensi dell'art. 37 del GDPR, l'ENS ha nominato quale Responsabile della Protezione dei Dati Personali (DPO - *Data Protection Officer*) l'Avv. Luca Sanna, contattabile all'indirizzo avv.lucasanna@gmail.com, il quale - ai sensi dell'art. 39 del GDPR - è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento Privacy UE 2016/679 (GDPR), nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del Regolamento Privacy UE 2016/679 (GDPR), di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Di seguito vengono riportate una serie di regole e di istruzioni, che devono essere osservate da ciascuna persona fisica preposta allo svolgimento delle operazioni di trattamento.

A) ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI, CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO.

- raccolta/profilazione: prima di procedere alla raccolta dei dati personali, deve essere fornita l'informativa all'interessato o alla persona della quale si raccolgono i dati. Occorre procedere alla raccolta dei dati con la massima cura, verificandone l'esattezza, nonché la pertinenza, la completezza e la non eccedenza rispetto alle finalità del trattamento, secondo quanto previsto dalla legge o dai regolamenti e le istruzioni del responsabile del la struttura;
- registrazione: non lasciare Cd-Rom, Dvd, fogli, cartelle e quant'altro a disposizione di estranei;

- conservazione: i documenti o gli atti che contengono dati di categoria particolari o "giudiziari" devono essere conservati in archivi ad accesso controllato, per cui occorre garantire che armadi, schedari e contenitori siano muniti di serratura ovvero che l'autorizzato del trattamento, che riceva cittadini e utenti, sia sempre presente nella propria stanza o luogo di lavoro, evitando che le informazioni trattate possano essere visualizzate e rese conoscibili a terzi. Sarà cura di ciascun responsabile del trattamento provvedere affinché venga escluso un accesso ad archivi e a dati da parte di soggetti che non siano autorizzati al trattamento;
- utilizzo: i dati possono essere utilizzati solo da coloro che sono stati espressamente autorizzati al trattamento. L'utilizzo dei dati deve avvenire solo per scopi determinati, espressi e legittimi e si deve evitare un utilizzo per scopi diversi rispetto a quello istituzionali dell'ente o non compatibili con gli stessi, con riferimento alle attività affidate e di competenza dell'unità di trattamento di appartenenza;
- blocco: questo può essere conseguenza di una espressa richiesta da parte dell'interessato ovvero può essere ordinato dal Garante per la protezione dei dati personali;
- comunicazione: con tale espressione, secondo quanto previsto dalla legge, si intende il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Ciò che caratterizza l'operazione di comunicazione è il fatto che, considerato il rapporto diretto tra titolare (ENS) e interessato (ad esempio un cittadino utente, un dipendente o un'impresa), un soggetto determinato (in posizione di terzietà rispetto a questo rapporto bilatero) possa in qualunque forma conoscere dati personali riferiti all'interessato medesimo;
- **comunicazione di dati cd. comuni**: qualora il richiedente i dati personali sia un soggetto pubblico, la comunicazione dei cd. dati comuni potrà avvenire, pur in mancanza di espressa previsione di legge o di regolamento, ove sia necessaria per l'esercizio di una finalità istituzionale dell'ente destinatario della comunicazione stessa. In tal caso, tuttavia, occorrerà segnalare la circostanza al proprio responsabile, affinché proceda alla comunicazione preventiva al Garante per la protezione dei dati personali;
- **comunicazione di categorie particolari di dati:** Tali dati possono essere comunicati a soggetti determinati solo ove sia espressamente previsto da una legge, che autorizzi tale operazione, in conformità al parere del Garante per la protezione dei dati personali;
- diffusione: per diffusione si intende il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. La pubblicazione di qualsiasi atto (all'albo pretorio o in una bacheca, ovvero in Internet), che contenga dati personali, costituisce una forma di diffusione di informazioni personali;
- **cancellazione**: l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento; l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; i dati personali sono stati trattati illecitamente; i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.
Qualora richiesta la cancellazione del dato e qualora terminata la finalità del trattamento, la documentazione deve essere distrutta con modalità che non permettano la ricostruzione del documento.
I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Reg. UE 2016/679.

B) ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI PER IL TRATTAMENTO.

-computer: tutte le volte che si abbandona la propria postazione di lavoro, il pc (o il terminale) in uso deve essere posto in condizione, per cui i dati non siano accessibili a estranei non autorizzati (si deve adottare uno screen saver con password ovvero sospendere la propria sessione di lavoro, disconnettendosi dall'applicazione in uso);

- email e uso dell'Internet: la posta elettronica deve essere utilizzata per scopi di ufficio. Si ricorda che qualunque comunicazione ricevuta o spedita utilizzando l'indirizzo di posta dell'ENS, non è corrispondenza personale dell'operatore, per cui potrebbero essere effettuati controlli remoti al fine di verificare l'uso improprio o illecito degli strumenti forniti in dotazione;

- protezione dei dati particolari: occorre fare particolare attenzione alla spedizione, a mezzo di posta elettronica, di file o di messaggi contenenti categorie particolari di dati. In tal caso, occorrerà proteggere il contenuto del file dall'accesso e dalla visione di soggetti non autorizzati o legittimati al trattamento, diversi dai destinatari delle comunicazioni elettroniche considerate. A titolo meramente esemplificativo, si consiglia (a seconda dei casi, da valutarsi a cura del responsabile del trattamento) il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero all'utilizzo di codici identificativi dell'identità dell'interessato associati ai dati particolari ovvero dati relativi a condanne penali o reati, in modo da rendere inintelligibili i dati in caso di intercettazione delle comunicazioni;

- file di log: per ragioni di sicurezza, si può avere la necessità di installare dispositivi automatizzati di registrazione delle operazioni svolte con elaboratori elettronici (cd. file di log) ovvero delle connessioni a Internet o dell'uso della posta elettronica;

- fax: questo strumento appare utile a garantire efficienza, economicità e velocità di comunicazione; tuttavia, presenta rischi specifici riguardo all'identità (a volte sconosciuta) di colui che materialmente riceve il documento trasmesso. A tal proposito, prima di inviare documenti contenenti categorie particolari di dati o per i quali vi siano esigenze di riservatezza, assicurarsi preventivamente che l'effettivo destinatario sia sul posto o comunque che non vi siano rischi di conoscenza del contenuto da parte di soggetti non autorizzati. Si consiglia di anticipare telefonicamente la trasmissione e di inserire in calce alla copertina del fax, che viene utilizzata per la spedizione della documentazione allegata, la seguente formula: "Qualora il destinatario del presente fax non sia la persona indicata nella presente copertina, è pregato di dare immediata comunicazione al mittente, a mezzo telefono o per fax. Successivamente, si prega di distruggere la documentazione erroneamente ricevuta, con l'avvertimento che in caso di non ottemperanza a questo invito si potrà essere responsabili della mancanza di protezione o dell'uso non autorizzato delle informazioni erroneamente acquisite";

- Istruzioni per l'utilizzo del fax:

- digitare correttamente il numero di telefono, cui inviare la comunicazione;
- controllare l'esattezza del numero digitato prima di inviare il documento;
- verificare che non vi siano inceppamenti della carta ovvero che non vengano presi più fogli contemporaneamente;
- attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
- qualora vengano trasmessi dati idonei a rivelare lo stato di salute, può essere opportuno anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
- in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;

- telefono: non fornire dati e informazioni di carattere personale o di natura comunque riservata per telefono, qualora non si conosca o non si abbia verosimilmente cognizione dell'identità o della legittimazione a conoscere del soggetto chiamante. In molti casi, si consiglia di richiedere l'identità del

chiamante e la qualità, quindi di provvedere a richiamare, avendo così la certezza sull'identità del richiedente;
- scanner: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;
- Pen-Drive: i supporti informatici, già utilizzati per il trattamento dei dati personali di qualunque tipologia, devono essere riutilizzati solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti. Tali dispositivi, qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura;
- cd-rom: i supporti informatici, già utilizzati per il trattamento dei dati possono essere riutilizzati solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti. Tali dispositivi, qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura;
- spedizione di documenti contenenti dati personali a mezzo posta: la documentazione contenente categorie particolari di dati ovvero dati relativi a condanne penali o reati, deve essere trasferita, anche all'interno delle Strutture aziendali, in busta chiusa, in modo da proteggere la riservatezza del documento e dei dati contenuti. I lembi della busta devono essere sigillati e firmati per garantire l'integrità del contenuto;
- uso di software: è vietato installare e usare qualunque software, anche se scaricato da internet, senza la previa autorizzazione da parte dell'amministratore di sistema. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito, sia di natura penale, sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs. 518/1992 e successive modificazioni e integrazioni;
- Connessione internet WI-FI: Quale misura che intenda incentivare l'utilizzo della rete Wi-Fi all'interno delle sedi ENS per ospiti e lavoratori e che al contempo impedisca il libero accesso alla rete si richiede ai responsabili delle sedi territoriali ovvero ai soggetti autorizzati del trattamento di creare ed allestire un hotspot dedicato.
È preferibile che l'utilizzo di tale hotspot avvenga per mezzo di una rete dedicata ovvero di uno strumento che possa permettere di verificare gli accessi, affinché il titolare dell'abbonamento Internet possa essere estraneo alla eventuale e possibile violazione commessa e dimostrare che qualcun altro ha utilizzato la sua connessione.

C) ULTERIORI ISTRUZIONI PER I SOGGETTI AUTORIZZATI AL TRATTAMENTO.

Le persone autorizzate devono, altresì, rispettare le istruzioni seguenti in tema di protezione e di sicurezza dei dati e degli strumenti nello svolgimento delle operazioni affidate:
Rapporti di front-office e gestione documenti cartacei:
- identificazione dell'interessato: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di verifica dell'identità della persona e garanzia di correttezza del dato da raccogliere; può essere quindi necessario richiedere e ottenere un documento di identità o di riconoscimento;
- controllo dell'esattezza del dato: fare attenzione alla digitazione ed all'inserimento dei dati identificativi e personali degli interessati, evitando errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel proseguo del processo;
- obbligo di riservatezza e segretezza: il soggetto autorizzato al trattamento ha l'obbligo della riservatezza e del segreto sulle informazioni, di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare la comunicazione o la diffusione delle informazioni a soggetti non autorizzati o che non abbiano necessità di conoscere i dati trattati;

- tenuta cartelle e fascicoli: cartelle e fascicoli tenuti sulla propria scrivania, qualora si ricevano nella propria stanza utenti e cittadini, devono essere trattati in modo da garantire la riservatezza degli interessati. Si consiglia di rivoltare sotto sopra le cartelle ovvero di inserire (a seconda delle necessità operative e organizzativi) sul frontespizio dati e informazioni per cui non sia resa conoscibile a terzi estranei l'identità dei soggetti interessati;
- distruzione delle copie cartacee: evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto: si potranno utilizzare apparati distruggi documenti o altri sistemi (ad esempio strappo dei documenti, separazione del dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli);
- **data breach:** i dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.
Per tale ragione il soggetto autorizzato venuto a conoscenza di una violazione o di una perdita del dato personale, anche in occasione di catastrofi naturali, deve senza indugio comunicare al proprio responsabile, se presente, ovvero al titolare del trattamento del dato personale la circostanza ed accertarsi che la problematica venga presa in carico (anche chiedendo una risposta per iscritto da parte del soggetto responsabile del trattamento dei dati personali). In calce al presente documento è stata dettagliata una guida completa da seguire in caso di *Data – Breach.*

D) ISTRUZIONI IN TEMA DI SICUREZZA DEGLI STRUMENTI ELETTRONICI.

a) parola chiave/login/dati accesso Cariddi: la parola chiave/login/dato accesso Cariddi, assegnata a ciascun incaricato, deve essere composta da un minimo di 4 caratteri o comunque dal numero massimo di caratteri consentito dal sistema.
Si raccomanda di cambiare la parola chiave del soggetto autorizzato al trattamento ogni sei mesi.
La password non deve contenere riferimenti agevolmente riconducibile all'autorizzato e dovrebbe essere generata preferibilmente senza un significato compiuto.
Il soggetto autorizzato, nello scegliere la propria password, deve preferibilmente utilizzare anche caratteri speciali e lettere maiuscole e minuscole.
La parola chiave deve essere custodita con la massima attenzione e segretezza e non deve essere comunicata a terzi, per alcun motivo o ragione.
Il soggetto autorizzato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare.
Ove vi sia la necessità di garantire la disponibilità dei dati e dei documenti a persone terze, deve essere richiesta l'abilitazione all'amministratore di sistema e ogni incaricato deve poter accedere con la propria credenziale di autenticazione.
b) back-up: salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno bisettimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati che siano messi a disposizione del soggetto autorizzato e consegnare i supporti contenenti le copie di salvataggio al responsabile della struttura, ovvero riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati.
c) antivirus: a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, i soggetti autorizzati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando venga segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza sull'elaboratore in dotazione di virus.

d) conservazione supporti rimovibili: i supporti utilizzati per la memorizzazione di copie di file di documenti di lavoro non devono essere lasciati in luoghi accessibili. Si consiglia di riporre cd-rom, DVD, dispositivi di memorizzazione in cassetti muniti di serratura ovvero di custodire gli stessi in modo da garantire un accesso controllato.
e) strumenti di comunicazione social e di sistemi di messaggistica istantanea: l'unico strumento ammesso per le comunicazioni tra i soggetti autorizzati al trattamento dei dati personali, responsabili e titolari del trattamento è la mai fornita dall'ente. I sistemi di messaggistica istantanea (*WhatsApp, Telegram, Viber, Skype,* Ecc..) e i social Network (*Facebook, Twitter, Linkedyn, ecc.*.) non sono strumenti sicuri per le comunicazioni dei dati personali e come tali possono essere utilizzati solamente quali strumenti personali di comunicazione.

E) DEFINIZIONE DATA BREACH - PROCEDURA DA SEGUIRE IN CASO DI DATA BREACH

L'art. 33 del GDPR recita che: "*In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 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*".
Per "*Data Breach*" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali". Nello specifico, l'articolo 4 p.12 del GPDR definisce la violazione dei dati personali come 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.
Ogni qual volta un soggetto incaricato dall'ENS come lavoratore/collaboratore/volontario venga a conoscenza di un episodio che possa mettere a repentaglio l'integrità o la riservatezza dei dati personali deve dare avviso al Responsabile Territoriale del Trattamento dei dati personali identificato con il Presidente/Commissario Straordinario e con il Responsabile del Trattamento scrivendo all'indirizzo privacy@ens.it senza indugio e nell'immediatezza del fatto, indicando nella comunicazione i seguenti elementi:

1. Nome e Cognome del soggetto che effettua la comunicazione
2. Recapiti telefonici e mail del soggetto che effettua la comunicazione
3. Funzione rivestita
4. Breve descrizione dei fatti che si presuma abbiano prodotto una violazione dei dati personali
5. Data e Luogo della presunta violazione.

A titolo esemplificativo si indicano di seguito alcuni esempi di *Data Breach*:

- Furto
- Accesso illecito di soggetti estranei all'interno dei locali ENS
- Computer colpito da virus (malware, hacker, phishing, ecc.)
- Incendio
- Alluvione
- Crash dei server interni
- Smarrimento di hard disk o di computer portatili
- Smarrimento di documenti, cartelle, faldoni contenenti dati personali.

APPENDICE COVID-19

Ai fini del contenimento e della gestione del virus COVID 19 negli ambienti di lavoro dell'ENS, la prosecuzione delle attività produttive dovrà nei fatti avvenire solo in presenza di condizioni che assicurino alle persone che lavorano adeguati livelli di protezione.
L' ENS ha inteso diffondere una corretta informazione, attraverso le modalità più idonee ed efficaci, informando tutti i lavoratori e chiunque entri in azienda circa le disposizioni delle Autorità, consegnando e/o affiggendo all'ingresso e nei luoghi maggiormente visibili dei locali aziendali, appositi *depliants* informativi al cui interno è rappresentato quanto segue:

- l'obbligo di rimanere al proprio domicilio in presenza di febbre (oltre 37.5°) o altri sintomi influenzali e di chiamare il proprio medico di famiglia e l'autorità sanitaria o la consapevolezza e l'accettazione del fatto di non poter fare ingresso o di poter permanere in azienda e di doverlo dichiarare tempestivamente laddove, anche successivamente all'ingresso, sussistano le condizioni di pericolo (sintomi di influenza, temperatura, provenienza da zone a rischio o contatto con persone positive al virus nei 14 giorni precedenti, ecc.) in cui i provvedimenti dell'Autorità impongono di informare il medico di famiglia e l'Autorità sanitaria e di rimanere al proprio domicilio;
- l'impegno a rispettare tutte le disposizioni delle Autorità e del datore di lavoro nel fare accesso in azienda (in particolare, mantenere la distanza di sicurezza, osservare le regole di igiene delle mani e tenere comportamenti corretti sul piano dell'igiene);
- l'impegno a informare tempestivamente e responsabilmente il datore di lavoro della presenza di qualsiasi sintomo influenzale durante l'espletamento della prestazione lavorativa, avendo cura di rimanere ad adeguata distanza dalle persone presenti.

In tal senso sino al termine dell'emergenza epidemiologica il personale, prima dell'accesso al luogo di lavoro potrà essere sottoposto al controllo della temperatura corporea. Se tale temperatura risulterà superiore ai 37,5°, non sarà consentito l'accesso ai luoghi di lavoro. Le persone in tale condizione – nel rispetto delle indicazioni riportate in nota – saranno momentaneamente isolate o allontanate.
La rilevazione in tempo reale della temperatura corporea costituisce un trattamento di dati personali e, pertanto, deve avvenire ai sensi della disciplina privacy vigente. A tal fine non verrà registrato alcun dato in merito alla temperatura corporea se non in casi di sospetto contagio al fine di comunicare la circostanza all'interessato, per poter permettere allo stesso le comunicazioni al proprio medico curante.
Si ricorda che i dati possono essere trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19 e non devono essere diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali "*contatti stretti di un lavoratore risultato positivo al COVID-19*").
In caso di isolamento momentaneo dovuto al superamento della soglia di temperatura, verranno assicurate modalità tali da garantire la riservatezza e la dignità del lavoratore. Tali garanzie saranno assicurate anche nel caso in cui il lavoratore comunichi all'ufficio responsabile del personale di aver avuto, al di fuori del contesto aziendale, contatti con soggetti risultati positivi al COVID-19 e nel caso di allontanamento del lavoratore che durante l'attività lavorativa sviluppi febbre e sintomi di infezione respiratoria e dei suoi colleghi.
Qualora si richieda il rilascio di una dichiarazione attestante la non provenienza dalle zone a rischio epidemiologico e l'assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al COVID-19, si provvederà a raccogliere i soli dati necessari, adeguati e pertinenti rispetto alla prevenzione del contagio da COVID-19, astenendosi nell'indicare i nominativi dei contatti risultati positivi al virus ed astenendosi nello specificare i luoghi di provenienza.