POLICY PRIVACY

ISTRUZIONI OPERATIVE, NORME DI COMPORTAMENTO E LINEE GUIDA PER LA GESTIONE ED IL RISPETTO DEL REGOLAMENTO EUROPEO 2016/679 PER LA PROTEZIONE DEI DATI PERSONALI E LE CORRETTE MODALITA' D'USO DI STRUMENTI AZIENDALI E RELATIVI CONTROLLI

INDICE

1. SCOPO

2. RIFERIMENTI NORMATIVI

3. CAMPO DI APPLICAZIONE E DEFINIZIONI

4. SOGGETTI

5. PRINCIPI E BASI GIURIDICHE DEL TRATTAMENTO

6. RISERVATEZZA

7. GLI STRUMENTI DI LAVORO. Istruzioni di utilizzo

8. IL RISPETTO DELLE MISURE DI SICUREZZA INFORMATICHE

9. VIOLAZIONE DI DATI PERSONALI

10. MODALITÀ DI SVOLGIMENTO DEI CONTROLLI

11. TRATTAMENTO SENZA STRUMENTI ELETTRONICI (DOCUMENTI CARTACEI)

12. LINEE GUIDA PER I DIPENDENTI SUI SOCIAL MEDIA

13. MODALITA' PER ELABORARE E CUSTODIRE LE PASSWORD

14. AGGIORNAMENTI PERIODICI

15. REFERENTI AZIENDALI

1. SCOPO

Il presente documento ha lo scopo di trasmettere la completa e corretta conoscenza delle modalità operative alle quali le persone autorizzate al trattamento dei dati personali, nominate per iscritto dal Titolare, devono attenersi per garantire il rispetto del "Regolamento Europeo in materia di protezione dei dati personali 2016/679 ", del Codice Privacy novellato dal D. Lgs 101/18, delle linee guida e dei provvedimenti emanati dalle autorità di controllo, nonchè delle misure tecniche ed organizzative adottate dal Titolare per garantire la riservatezza, l'integrità e la disponibilità dei dati.

Il mancato rispetto delle modalità operative descritte nel presente documento può comportare:

- responsabilità penale in caso di mancata adozione delle misure di sicurezza;
- responsabilità civile nei confronti dei terzi danneggiati a seguito del trattamento illecito dei dati;
- responsabilità per inadempienza contrattuale nei confronti del Titolare del trattamento;
- responsabilità nei confronti del titolare per violazioni relative al rapporto di lavoro e conseguenti rapporti disciplinari o richieste di risarcimento/rivalsa.

2. RIFERIMENTI NORMATIVI

Regolamento Europeo in materia di protezione dei dati personali 2016/679; Codice Privacy novellato da D. Lgs 101/18; Provvedimenti e Linee guida delle autorità di controllo (italiana ed europea); art. 4, Legge 300 del 20/05/1970 come modificato dall'art. 23 del D.lgs. 81 del 23/09/2015.

3. CAMPO DI APPLICAZIONE E DEFINIZIONI

Il presente documento si applica alle modalità di trattamento di tutti i dati personali, al fine di garantire, così come indicato dall'art. 1, 2 e 3 del Regolamento Europeo 2016/679, che il trattamento stesso si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della

dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

A tal fine si ricorda che s'intende per:

- **TRATTAMENTO:** QUALSIASI OPERAZIONE O INSIEME DI OPERAZIONI, COMPIUTE CON O SENZA L'AUSILIO DI PROCESSI AUTOMATIZZATI E APPLICATE A DATI PERSONALI O INSIEMI DI DATI PERSONALI, COME LA RACCOLTA, LA REGISTRAZIONE, L'ORGANIZZAZIONE, LA STRUTTURAZIONE, LA CONSERVAZIONE, L'ADATTAMENTO O LA MODIFICA, L'ESTRAZIONE, LA CONSULTAZIONE, L'USO, LA COMUNICAZIONE (MEDIANTE TRASMISSIONE, DIFFUSIONE O QUALSIASI ALTRA FORMA), IL RAFFRONTO O L'INTERCONNESSIONE, LA LIMITAZIONE, LA CANCELLAZIONE O LA DISTRUZIONE (REGOLAMENTO EUROPEO 2016/679 ART. 4 COMMA 2);
- **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 IL NOME, IL DOMICILIO O UNO O PIÙ ELEMENTI CARATTERISTICI DELLA SUA IDENTITÀ FISICA, FISIOLOGICA, GENETICA, PSICHICA, ECONOMICA, CULTURALE O SOCIALE (REGOLAMENTO EUROPEO 2016/679 ART. 4 COMMA 1).
- **DATI GENETICI:** I DATI PERSONALI RELATIVI ALLE CARATTERISTICHE GENETICHE DI UNA PERSONA FISICA (EREDITARIE O ACQUISITE) CHE FORNISCONO INFORMAZIONI UNIVOCHE SULLA FISIOLOGIA O SULLA SALUTE DI DETTA PERSONA E CHE RISULTANO, IN PARTICOLARE, DALL'ANALISI DI UN CAMPIONE BIOLOGICO DELLA PERSONA FISICA IN QUESTIONE (REGOLAMENTO EUROPEO 2016/679 ART. 4 COMMA 13)
- **DATI BIOMETRICI**: I DATI PERSONALI OTTENUTI DA UN TRATTAMENTO TECNICO SPECIFICO RELATIVI ALLE CARATTERISTICHE FISICHE, FISIOLOGICHE O COMPORTAMENTALI DI UNA PERSONA FISICA CHE NE CONSENTONO O CONFERMANO L'IDENTIFICAZIONE UNIVOCA, QUALI L'IMMAGINE FACCIALE O I DATI DATTILOSCOPICI (REGOLAMENTO EUROPEO 2016/679 ART. 4 COMMA 14);
- **DATI RELATIVI ALLA SALUTE**: I DATI PERSONALI ATTINENTI ALLA SALUTE FISICA O MENTALE DI UNA PERSONA FISICA, COMPRESA LA PRESTAZIONE DI SERVIZI DI ASSISTENZA SANITARIA, CHE RIVELINO INFORMAZIONI RELATIVE AL SUO STATO DI SALUTE (REGOLAMENTO EUROPEO 2016/679 ART. 4 COMMA 15)
- **TRATTAMENTO DI CATEGORIE DI DATI PARTICOLARI:** I DATI PERSONALI CHE RIVELINO L'ORIGINE RAZZIALE O ETNICA, LE OPINIONI POLITICHE, LE CONVINZIONI RELIGIOSE O FILOSOFICHE, L'APPARTENENZA

SINDACALE, NONCHÉ DATI GENETICI, DATI BIOMETRICI INTESI AD IDENTIFICARE, IN MODO UNIVOCO, UNA PERSONA FISICA; DATI RELATIVI ALLA SALUTE O ALLA VISTA SESSUALE O ALL'ORIENTAMENTO SESSUALE DELLA PERSONA; DATI ATTINENTI ALLA SALUTE FISICA O MENTALE DI UNA PERSONA, COMPRESA LA PRESTAZIONE DI SERVIZI DI ASSISTENZA SANITARIA, CHE RILEVANO INFORMAZIONI RELATIVE AL SUO STATO DI SALUTE (REGOLAMENTO EUROPEO 2016/679 ART. 9 COMMA 1);

- **TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALE E REATI:** I DATI PERSONALI RELATIVI A CONDANNE PENALI E AI REATI (REGOLAMENTO EUROPEO 2016/679 ART.10);
- **PROFILAZIONE:** QUALSIASI FORMA DI TRATTAMENTO AUTOMATIZZATO DI DATI PERSONALI CONSISTENTE NELL'UTILIZZO DI DATI AL FINE DI VALUTARE DETERMINATI ASPETTI RELATIVI AD UNA PERSONA FISICA, CON PARTICOLARE RIFERIMENTO AL RENDIMENTO PROFESSIONALE, ALLA SITUAZIONE ECONOMICA, ALLA SALUTE, ALLE PREFERENZE PERSONALI, AGLI INTERESSI, ALL'AFFIDABILITÀ, AL COMPORTAMENTO, ALL'UBICAZIONE O AGLI SPOSTAMENTI DI DETTA PERSONA FISICA (REGOLAMENTO EUROPEO 2016/679 ART. 4 COMMA 4).

4. SOGGETTI

I Soggetti previsti dalla normativa a tutela dei dati personali e, pertanto, sottoposti alle Responsabilità riscontrabili nell'ambito del presente documento sono:

- Titolare del Trattamento dei dati personali (di seguito anche Azienda);
- Responsabili del Trattamento dei dati personali;
- Persone autorizzate al Trattamento dei dati personali;
- Amministratore di sistema.

Titolare del trattamento dei dati personali : 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 dei 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 (Regolamento Europeo 2016/679 art. 4 comma 7);

Responsabile del trattamento dei dati personali: la persona fisica, la persona giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (Regolamento Europeo 2016/679 art. 4 comma 8; Art 28);

Persone autorizzate al trattamento dei dati personali: le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare (Regolamento Europeo 2016/679 art. 4 comma 10);

Amministratore di sistema: le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (provvedimento del Garante per la protezione dei dati personali datato 27 novembre 2008 - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di IT - pubblicato sulla G.U. del 24 dicembre 2008, così come modificato dal successivo provvedimento del 25 Giugno 2009);

5. PRINCIPI E BASI GIURIDICHE DEL TRATTAMENTO

5.1. Principi del Trattamento

I dati personali devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non siano incompatibili con tali finalità; un trattamento dei dati finalizzato all'archiviazione per pubblici interessi, alla ricerca scientifica, storica o statistica non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente per finalità di archiviazione per pubblici interessi, per scopi di ricerca scientifica, storica o statistica, conformemente all'articolo 89, paragrafo 1 e fatta salva l'attuazione di misure tecniche e organizzative a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera tale da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati/illeciti/situazioni di perdita, distruzione o danno accidentale («integrità e riservatezza»).

5.2 Liceità del trattamento: basi giuridiche

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti o le libertà fondamentali dell'interessato che richiedano la protezione dei dati personali, in particolare se l'interessato è un minore.

6. RISERVATEZZA

Anche informazioni di normale quotidianità aziendale o ritenute non riservate da persone autorizzate al trattamento/lavoratori, assumono diversa importanza, e quindi richiedono una maggiore tutela, se comunicate all'esterno a soggetti terzi oppure se inserite su pagine di social network. La salvaguardia delle informazioni e dei dati, oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo aziendale, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni, è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno, o inserire su social network, qualsiasi informazione relativa al contenuto e all'attendibilità dell'interlocutore. Si precisa che, qualora nell'espletamento delle mansioni conferite alla persona autorizzata al trattamento/lavoratore, quest'ultima dovesse, anche accidentalmente o attraverso i colleghi, avere notizia o venire a conoscenza di dati, documenti, informazioni o notizie riguardanti l'organizzazione, l'attività e/o il know-how specifico dell'Azienda, queste - fatte salve le notizie o le informazioni che siano o divengano di dominio pubblico - sono da considerarsi oltre che di esclusiva proprietà aziendale, anche a carattere assolutamente riservato. Pertanto, sia nel corso dell'espletamento dell'incarico/prestazione lavorativa presso l'Azienda che dopo la scadenza dello stesso, la persona autorizzata al trattamento/lavoratore è tenuta a mantenere il più rigoroso riserbo sulle suddette informazioni, notizie e dati, e a non divulgarle o renderle in alcun modo disponibili a terzi. E' fatto divieto a tutte le persone autorizzate al trattamento di conservare, commercializzare, divulgare, trasmettere a terzi, in qualsivoglia forma, i dati aziendali, a meno che non sia necessario allo svolgimento delle mansioni affidate a ciascun interessato.

E' utile sapere che:

- per **social engineering** si intende l'insieme delle tecniche psicologiche utilizzate per indurre il soggetto autorizzato al trattamento dei dati/lavoratore alla raccolta di informazioni o dati (anche molto riservati) riguardanti l'azienda, l'organizzazione o il personale che vi lavora. Con l'ausilio di messaggi studiati o abili tecniche di persuasione

l'aggressore, infatti, può acquisire informazioni oppure ottenere l'apertura di allegati infetti o la visita ad un sito che contiene dialer o altro materiale pericoloso.

- per **email - phishing** si intende ugualmente l'insieme delle tecniche psicologiche con cui l'aggressore induce il soggetto autorizzato al trattamento dei dati/lavoratore ad aprire un'email e eseguire le istruzioni impartite (è il caso dell'invio di false comunicazioni email aventi grafica, forma, autorevolezza e logo ufficiale di Enti/Banche/Assicurazioni/Intermediari noti al pubblico). Nella maggior parte dei casi, l'aggressore, attraverso questa modalità, richiede la compilazione di moduli specifici e l'inserimento di informazioni riservate (come password, numero di carta di credito, ecc..).

COSA FARE

- non fornire informazioni confidenziali (al telefono o di persona) a interlocutori non conosciuti;
- fornire informazioni a interlocutori noti e operanti nel medesimo contesto aziendale, limitatamente ai contenuti afferenti l'ambito lavorativo assegnato;
- diffidare da messaggi provenienti da fonte non conosciuta;
- non aprire messaggi provenienti da fonte non conosciuta contenenti allegati;
- non aprire messaggi contenenti allegati sospetti;
- non trasmettere alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
- non trasmettere alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) poichè tali strutture non richiedono mai l'inserimento di dati utilizzando queste modalità;
- verificare sempre o in caso di dubbio l'attendibilità delle richieste ricevute con il Responsabile o il Titolare.

7. GLI STRUMENTI DI LAVORO. Istruzioni di utilizzo

Il Titolare, in riferimento al Provvedimento dell'01.03.2007 pubblicato sulla G.U.R.I. del 10.03.2007, n. 58, avente ad oggetto "Trattamento dei dati personali relativo all'utilizzo di

strumenti elettronici da parte dei lavoratori", all'art. 4, co. 2, L. 300/70 (strumenti di lavoro aziendali), Reg.to EU 2016/679, Codice privacy novellato dal D. Lgs 101/18 e altre fonti normative vigenti ed applicabili, impartisce alle persone autorizzate le seguenti istruzioni:

Posta elettronica

Alla persona autorizzata al trattamento, per lo svolgimento delle mansioni assegnate, viene attribuita una casella di posta elettronica aziendale. La stessa deve e dovrà essere utilizzata per finalità esclusivamente riconducibili allo svolgimento dell'attività lavorativa della persona autorizzata al trattamento. Il sistema di posta elettronica utilizzato è Office365 con applicativo Outlook.

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- Il dominio (lazzarospallanzani.it) al quale è collegato un servizio di posta e la relativa casella (es.: mario.rossi@lazzarospallanzani.it) è di proprietà aziendale; non è consentito, per fini lavorativi, utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai dominii aziendali;
- la durata della password per accedere alla casella di posta e per garantire la sicurezza dei dati è di 3 mesi (termine ritenuto congruo dall'IT); per la scelta della password, il sistema fornisce indicazioni utili (di lunghezza e caratteri da utilizzare) al punto 13);
- lo scambio di allegati contenenti dati particolari (art. 9) o giudiziari (art.10) - es: i dati sulla salute, dati relativi a condanne penali o reati - deve avvenire utilizzando canali sicuri: pec o modalità .rar o .zip con Password. E' opportuno, in caso di necessità, rivolgersi all' Responsabile dell'Ufficio Marketing o all'IT esterno per le dovute indicazioni;
- sono attivi indirizzi di posta elettronica condivisi da più operatori (es.: info@lazzarospallanzani.it , commerciale@lazzarospallanzani.it ; odontoiatria@lazzarospallanzani.it ; appuntamento@lazzarospallanzani.it ; laboratorio@lazzarospallanzani.it , ecc…) le cui credenziali di accesso sono conosciute da più persone;

- alla singola persona autorizzata al trattamento può essere assegnato un indirizzo e-mail personale del tipo: nome.cognome@xxx.it; in questo caso le credenziali sono strettamente personali e non cedibili;

La "personalizzazione" dell'indirizzo non comporta la proprietà o l'usufrutto in capo alla persona autorizzata al trattamento e la liceità di un utilizzo personale; trattasi di strumenti di lavoro di esclusiva proprietà aziendale messi a disposizione della persona autorizzata al solo fine di consentire un adeguato svolgimento delle proprie mansioni lavorative.

La persona autorizzata al trattamento deve partecipare attivamente alla gestione della privacy aziendale anche segnalando alla Direzione eventuali non conformità, evidenze di pericoli e/o tentativi di intrusione, cambiamenti delle mansioni, ecc.

Istruzioni per il servizio di posta elettronica in caso di prolungata assenza

Quando una persona autorizzata al trattamento è a conoscenza preventivamente di un'assenza per ferie, maternità (ecc...) deve attivare il risponditore automatico con l'out of office e indicare un indirizzo email o un nr. di telefono alternativo a cui fare riferimento.

Istruzioni per il servizio di posta elettronica in caso di assenza improvvisa

La persona autorizzata che, improvvisamente, si sia assentata deve contattare (direttamente o per il tramite dei propri referenti) l'IT esterno affinchè possa, in ogni momento, accedere alle sue impostazioni di posta elettronica, attivare il risponditore automatico con l'out of office e indicare un indirizzo email o un nr. di telefono alternativo a cui fare riferimento. Tutto ciò per consentire il normale svolgimento dell'attività lavorativa dell'azienda. La persona autorizzata al trattamento contestualmente riceverà informazioni sull'accesso e sulle modalità per modificare, al rientro, la password.

Istruzioni per il servizio di posta elettronica in caso di cessazione di attività lavorativa

L'Azienda provvede tempestivamente a disattivare l'account e, nel caso lo ritiene opportuno, ad attivare il risponditore automatico (che informa il mittente che la persona autorizzata al trattamento non fa più parte dell'organizzazione aziendale) e l'inoltra copia della posta aziendale alla persona incaricata di svolgere le medesime funzioni del lavoratore dimesso.

L'Azienda, inoltre, ha facoltà di verificare per esigenze lavorative, anche a ritroso, il contenuto della posta aziendale (che si ricorda non essere personale e nemmeno privata).

L'utilizzo di Internet

La persona autorizzata al trattamento dei dati/lavoratore può accedere ad Internet solo nei limiti dello svolgimento delle Sue mansioni.

Le persone autorizzate al trattamento dei dati personali ricevono le istruzioni di seguito indicate:

- NON È CONSENTITO NAVIGARE IN SITI NON ATTINENTI ALLO SVOLGIMENTO DELLE MANSIONI ASSEGNATE;
- NON È CONSENTITO NAVIGARE IN SITI CHE ACCOLGONO CONTENUTI CONTRARI ALLA MORALE E ALLE PRESCRIZIONI DI LEGGE;
- NON È CONSENTITO NAVIGARE IN SITI CHE POSSANO RIVELARE UNA PROFILAZIONE DELL'INDIVIDUO DEFINITA 'PARTICOLARE' AI SENSI DEL REGOLAMENTO EUROPEO 2016/679: IN PARTICOLARE SITI LA CUI NAVIGAZIONE PALESI ELEMENTI ATTINENTI ALLA FEDE RELIGIOSA, ALLE OPINIONI POLITICHE E SINDACALI O ALLE SUE ABITUDINI SESSUALI;
- NON È CONSENTITA L'EFFETTUAZIONE DI OGNI GENERE DI TRANSAZIONE FINANZIARIA IVI COMPRESE LE OPERAZIONI DI REMOTE BANKING, ACQUISTI ON-LINE E SIMILI, SALVO NEL CASO IN CUI SIA NECESSARIO PER L'ESPLETAMENTO DELLA PROPRIA ATTIVITÀ LAVORATIVA, OPPURE AUTORIZZATI DAL TITOLARE;
- NON È CONSENTITO LO SCARICO DI SOFTWARE GRATUITI TRIAL, FREEWARE E SHAREWARE PRELEVATI DA SITI INTERNET, SE NON ESPRESSAMENTE AUTORIZZATO DAL TITOLARE O DALL'IT;
- NON È CONSENTITO LO SCARICO DI MATERIALE ELETTRONICO TUTELATO DALLE NORMATIVE SUL DIRITTO D'AUTORE (SOFTWARE, FILE AUDIO, FILM, ETC.) NÉ ATTRAVERSO INTERNET NÉ ATTRAVERSO SERVIZI DI PEER TO PEER;
- È VIETATA OGNI FORMA DI REGISTRAZIONE A SITI I CUI CONTENUTI NON SIANO LEGATI ALL'ATTIVITÀ LAVORATIVA;
- NON È PERMESSA LA PARTECIPAZIONE, PER MOTIVI NON PROFESSIONALI, A FORUM E GIOCHI IN RETE PUBBLICA, NONCHE' L'UTILIZZO DI CHAT ONLINE, DI BACHECHE ELETTRONICHE E DI REGISTRAZIONI IN GUEST BOOK (ANCHE UTILIZZANDO PSEUDONIMI O NICKNAMES);

- NON È CONSENTITA LA MEMORIZZAZIONE DI DOCUMENTI INFORMATICI DI NATURA OLTRAGGIOSA E/O DISCRIMINATORIA PER SESSO, LINGUA, RELIGIONE, RAZZA, ORIGINE ETNICA, OPINIONE E APPARTENENZA SINDACALE E/O POLITICA.

Altri strumenti di lavoro

Il Personal computer (fisso o portatile), lo smartphone, i tablet ed i relativi programmi e/o applicazioni affidati alla persona autorizzata al trattamento sono, come è noto, strumenti di lavoro, pertanto:

- TALI STRUMENTI DEVONO ESSERE CUSTODITI IN MODO APPROPRIATO E CON LA CURA DEL BUON PADRE DI FAMIGLIA;
- TALI STRUMENTI POSSONO ESSERE UTILIZZATI SOLO PER FINI PROFESSIONALI (IN RELAZIONE ALLE MANSIONI ASSEGNATE), NON PER SCOPI PERSONALI, TANTOMENO PER SCOPI ILLECITI O PER SCOPI CHE NON ABBIANO ATTINENZA CON LA PROPRIA ATTIVITÀ LAVORATIVA, SE NON ESPRESSAMENTE AUTORIZZATI DAL TITOLARE DEL TRATTAMENTO;
- IL FURTO, IL DANNEGGIAMENTO O LO SMARRIMENTO DI TALI STRUMENTI DEVONO ESSERE PRONTAMENTE SEGNALATI ALL'AZIENDA;
- GLI APPARECCHI TELEFONICI (NUMERI DIRETTI DEGLI INTERNI ED UFFICI E DEL CENTRALINO) SONO SERVIZI AZIENDALI (MEZZI); I PC PORTATILI/FISSI, GLI SMARTPHONE E I TABLET SONO MEZZI AZIENDALI (MEZZI);
- L'UTILIZZO DI TALI MEZZI È CONCESSO PER L'ESPLETAMENTO O COMPLETAMENTO DELLE ATTIVITÀ LAVORATIVE CUI LA PERSONA AUTORIZZATA AL TRATTAMENTO/LAVORATORE È STATA PREPOSTA;
- GLI STRUMENTI AZIENDALI DEVONO ESSERE RESTITUITI ALL'AZIENDA STESSA NEL MOMENTO IN CUI NE FACCIA RICHIESTA;
- PER RAGIONI ORGANIZZATIVE, PRODUTTIVE, DI SICUREZZA DEL LAVORO E TUTELA DEL PATRIMONIO, E A SEGUITO DI CESSAZIONE DELL'ATTIVITÀ LAVORATIVA, LE PERSONE AUTORIZZATE DAL TITOLARE POSSONO ACCEDERE A TUTTI I DATI, AI BACK UP DEI DATI DEGLI STRUMENTI DI LAVORO IN DOTAZIONE AGLI ADDETTI, INCLUSE LE CARTELLE DI RETE. IN CASO DI TRATTAMENTO ILLECITO DI DATI (ES: CONSERVAZIONE SULLO STRUMENTO AZIENDALE DI DATI AD USO PERSONALE) QUESTI VERRANNO ELIMINATI DALLA PERSONA AUTORIZZATA. SI RICORDA, INFATTI, CHE GLI STRUMENTI AZIENDALI NON SONO PERSONALI E NEMMENO PRIVATI.

Ai fini sopra esposti sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni come, ad esempio, quelli qui di seguito richiamati a titolo indicativo.

Onde evitare il grave pericolo di introdurre virus Informatici nonché di alterare la stabilità delle applicazioni dei server si specifica quanto segue:

- È CONSENTITO INSTALLARE PROGRAMMI PROVENIENTI DALL'ESTERNO SOLO SE ESPRESSAMENTE AUTORIZZATI DALL' IT;
- NON È CONSENTITO INSTALLARE SOFTWARE (CON LICENZA O FREEWARE). IN CASI PARTICOLARI, DEVE ESSERE PREVENTIVAMENTE RICHIESTA L'AUTORIZZAZIONE ALL'IT CHE POTRÀ, EVENTUALMENTE, PROCEDERE SOLO DOPO ADEGUATE VERIFICHE;
- NON È CONSENTITO L'USO DI PROGRAMMI NON DISTRIBUITI UFFICIALMENTE PER SCARICARE SOFTWARE, MUSICA, FILM, (ECC...) SE COPERTI DA DIRITTO D'AUTORE;
- NON È CONSENTITO UTILIZZARE STRUMENTI SOFTWARE E/O HARDWARE ATTI AD INTERCETTARE, FALSIFICARE, ALTERARE O SOPPRIMERE IL CONTENUTO DI COMUNICAZIONI E/O DOCUMENTI INFORMATICI;
- NON È CONSENTITO MODIFICARE LE CONFIGURAZIONI IMPOSTATE SUGLI STRUMENTI DI LAVORO AZIENDALI;
- NON È CONSENTITA L'INSTALLAZIONE SUL PROPRIO PC DI MEZZI DI COMUNICAZIONE PROPRI (COME AD ESEMPIO CHIAVETTE INTERNET, ECC...);
- SUI PC DOTATI DI SCHEDA AUDIO E/O DI LETTORE CD E/O DVD NON È CONSENTITO L'ASCOLTO DI PROGRAMMI, FILES AUDIO O MUSICALI, SE NON PER FINALITA' PRETTAMENTE LAVORATIVE;
- È VIETATO SALVARE SUGLI STRUMENTI AZIENDALI (PC AZIENDALI, SMARTPHONE E TABLET) DATI DI CARATTERE PERSONALE. IL PC, LO SMARTPHONE ED IL TABLET DEVONO ESSERE UTILIZZATI SOLO ED ESCLUSIVAMENTE PER LO SVOLGIMENTO DELL'ATTIVITÀ LAVORATIVA; SI RICORDA CHE DURANTE LE ORE LAVORATIVE È VIETATO OCCUPARSI DI COSE ESTRANEE AL SERVIZIO SVOLTO PER CONTO DELL'AZIENDA;
- NON È CONSENTITO SALVARE DATI AZIENDALI SUI SUPPORTI ESTERNI (CHIAVETTE USB, CD, DVD, UNITÀ ESTERNE ECC.);
- NON È ASSOLUTAMENTE CONSENTITO SALVARE I DATI AZIENDALI CHE RIGUARDANO LA SALUTE DEGLI INTERESSATI SU PIATTAFORME ESTERNE (DROPBOX, CLOUD O SIMILARI) SE NON ESPRESSAMENTE AUTORIZZATI DALL' IT;

- NON È ASSOLUTAMENTE CONSENTITO EFFETTUARE TRASMISSIONI TELEMATICHE NON AUTORIZZATE DI DATI OGGETTO DEL TRATTAMENTO;
- È VIETATO USARE I PC AZIENDALI, GLI SMARTPHONE, I TABLET E I PROGRAMMI IN ESSI INSTALLATI PER USO EXTRA LAVORATIVO;
- NEL CASO IN CUI LA PERSONA AUTORIZZATA AL TRATTAMENTO/LAVORATORE FOSSE AUTORIZZATO AD UTILIZZARE PER LO SVOLGIMENTO DELLA PROPRIA ATTIVITÀ LAVORATIVA IL PERSONAL COMPUTER PERSONALE O ALTRI STRUMENTI PERSONALI (ES SMARTPHONE, TABLET, SUPPORTI ESTERNI), SI PRECISA CHE QUESTO DOVRA' GARANTIRE, SOTTO LA SUA ESCLUSIVA RESPONSABILITA', CHE TALI DISPOSITIVI SIANO DOTATI DI VISURE TECNICHE IDONEE PER PROTEGGERE I TRATTAMENTI DI DATI DI CUI E' TITOLARE L'AZIENDA. UNA VIOLAZIONE DI DATI DEL TITOLARE DEVE ESSERE PRONTAMENTE COMUNICATA ALLA DIREZIONE (IN CASO DI COMUNICAZIONE TARDIVA, LA PERSONA AUTORIZZATA DOVRA' RISPONDERE CON ADEGUATE MOTIVAZIONI).

Supporti Magnetici

- NON È CONSENTITO SCARICARE FILES CONTENUTI IN SUPPORTI MAGNETICI/OTTICI NON AVENTI ALCUNA ATTINENZA CON LA PROPRIA PRESTAZIONE LAVORATIVA;
- TUTTI I FILES DI PROVENIENZA INCERTA O ESTERNA, ANCORCHÉ ATTINENTI ALL'ATTIVITÀ LAVORATIVA, DEVONO ESSERE SOTTOPOSTI AL CONTROLLO E RELATIVA AUTORIZZAZIONE ALL'UTILIZZO DA PARTE DELL' IT;
- LE UNITÀ DI RETE SONO AREE DI CONDIVISIONE DI INFORMAZIONI STRETTAMENTE PROFESSIONALI E NON POSSONO, IN ALCUN MODO, ESSERE UTILIZZATE PER SCOPI DIVERSI. PERTANTO, QUALUNQUE FILES CHE NON SIA LEGATO ALL'ATTIVITÀ LAVORATIVA NON PUÒ ESSERE DISLOCATO, NEMMENO PER BREVI PERIODI, IN QUESTE UNITÀ; L'AZIENDA SI RISERVA LA FACOLTÀ DI PROCEDERE ALLA RIMOZIONE DI OGNI FILES O APPLICAZIONE CHE RITERRÀ ESSERE PERICOLOSA PER LA SICUREZZA DEL SISTEMA OVVERO ACQUISITI O INSTALLATI IN VIOLAZIONE DELLE PRESENTI ISTRUZIONI.

Strumenti di lavoro elettronici portatili

Qualora per lo svolgimento del trattamento dei dati personali, la persona autorizzata al trattamento si trovasse ad utilizzare strumenti elettronici portatili, quali personal computer,

smartphone e tablet, dovranno essere rispettate tutte le indicazioni menzionate nei punti precedenti e nelle norme aggiuntive sull'utilizzo dei device mobili. Dovrà, inoltre, essere posta particolare attenzione a quelli che possono essere i potenziali rischi per i dati personali come smarrimenti, furti, cadute accidentali e perdite fortuite di dati, ecc.. Si raccomanda pertanto la massima cautela e cura nello svolgimento delle operazioni di trattamento dati contenuti in strumenti di lavoro personali.

Device mobili (smartphone e tablet) aziendali e personali.

Le presenti norme hanno lo scopo di sensibilizzare le persone autorizzate al trattamento dei dati personali per garantire un buon livello di sicurezza delle informazioni, sia aziendali che personali. Le istruzioni fornite in questo punto sono degli ottimi suggerimenti che non vogliono limitare l'utilizzo del device, ma che si rendono necessarie per garantire un buon livello di salvaguardia delle informazioni e dei dati presenti sui device mobili aziendali.

Device Aziendali

Istruzioni comportamentali per gli utilizzatori di device aziendali

1. il dispositivo viene messo a disposizione dall'Azienda per il tempo e l'uso determinato dalla mansione ricoperta, con l'obbligo di custodirlo con diligenza e renderlo alla scadenza nello stato originario, fatto salvo il deterioramento fisiologico risultante dall'uso normale dello stesso;
2. il dispositivo non deve essere lasciato incustodito e/o accessibile a terzi durante una sessione di trattamento. Non disattivare il blocco del dispositivo impostato;
3. il Titolare non è responsabile per il contenuto veicolato attraverso gli strumenti assegnati, né degli usi impropri che ne potrebbero essere fatti;
4. il consumo rientra nei limiti di utilizzo assegnati alla singola persona autorizzata al trattamento/lavoratore;
5. non deve essere utilizzato come hot spot per scopi personali;
6. evitare di installare o utilizzare APP che possano raccogliere dati presenti sul device, siano queste gratuite o a pagamento;

7. eseguire, almeno annualmente, gli aggiornamenti periodici dei programmi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti. Lo strumento è stato impostato per eseguire gli aggiornamenti periodici forniti dal produttore;
8. non navigare su siti che possono rivelare le opinioni sessuali, politiche, religiose, sindacali, pedopornografici, pornografici (ecc…);
9. è vietato scaricare materiale e programmi in violazione della legislazione sul diritto d'autore (es scarico musica, film gratuiti).

L'IT esterno si occuperà di configurare il PC portatile con tutte le visure di sicurezza previste dal Titolare. Relativamente all'assegnazione di smartphone aziendali, la persona autorizzata deve garantire, sotto la sua esclusiva responsabilità, che tali dispositivi siano dotati di visure tecniche idonee per proteggere i dati di cui è titolare l'azienda (es:. PIN; antivirus; blocco del dispositivo da remoto). Se si necessita di assistenza per la configurazione, è possibile rivolgersi all'IT esterno. Una violazione di dati (es: smarrimento del dispositivo, accesso non autorizzato, ecc…) deve essere prontamente comunicata alla Direzione (in caso di comunicazione tardiva, la persona autorizzata dovrà rispondere con adeguate motivazioni).

Device Personali

Istruzioni comportamentali per gli utilizzatori di device personali

Alcune persone autorizzate al trattamento dei dati personali sono state autorizzate ad accedere alla posta elettronica con strumenti di proprietà personale. Oltre a quanto indicato nel presente documento, la persona autorizzata al trattamento deve garantire, sotto la sua esclusiva responsabilità, che tali dispositivi siano dotati di visure tecniche idonee per proteggere i trattamenti di dati di cui è titolare l'azienda (es:. PIN; antivirus; blocco del dispositivo da remoto). Se si necessita di assistenza per la configurazione, è possibile rivolgersi all'IT esterno. Una violazione di dati (es: smarrimento del dispositivo, accesso non autorizzato, ecc…) deve essere prontamente comunicata alla Direzione (in caso di comunicazione tardiva, la persona autorizzata dovra' rispondere con adeguate motivazioni).

In particolare si consiglia di adottare le seguenti indispensabili istruzioni:

- NON LASCIARE MAI INCUSTODITO O ACCESSIBILE LO STRUMENTO DI PROPRIETÀ PERSONALE MENTRE È ATTIVA UNA SESSIONE DI LAVORO. ATTIVARE PERTANTO IL BLOCCO DELLO STRUMENTO DOPO UN BREVE PERIODO DI INUTILIZZO;
- SUL DEVICE INSTALLARE E ATTIVARE IL SOFTWARE ANTIVIRUS E FIREWALL GENERALMENTE FORNITO O COMUNQUE INDICATO DALLA STESSA CASA PRODUTTRICE. TALI SOFTWARE DEVONO ESSERE COSTANTEMENTE AGGIORNATI A CURA DELLA PERSONA AUTORIZZATA AL TRATTAMENTO;
- EFFETTUARE, ALMENO ANNUALMENTE, GLI AGGIORNAMENTI PERIODICI DEI PROGRAMMI VOLTI A PREVENIRE LA VULNERABILITÀ DI STRUMENTI ELETTRONICI E A CORREGGERNE DIFETTI. IN CASO DI TRATTAMENTO DI DATI SULLA SALUTE, PARTICOLARI O RELATIVI A CONDANNE PENALI E REATI, L'AGGIORNAMENTO È ALMENO SEMESTRALE. SULLO STRUMENTO DEVONO ESSERE QUINDI IMPOSTATI GLI AGGIORNAMENTI PERIODICI FORNITI DAL PRODUTTORE;
- NON SCARICARE DATI DI NESSUNA NATURA AZIENDALE ALL'INTERNO DEI DISPOSITIVI PERSONALI;
- NON ATTIVARE IL BACK UP O IL CLOUD STORAGE AUTOMATICO QUALORA SIANO PRESENTI DATI AZIENDALI. IL BACK UP DEI DATI AZIENDALI DEVE ESSERE EFFETTUATO SOLO SU SERVER AZIENDALI E/O SULLA RUBRICA DI POSTA AZIENDALE;
- NON SCARICARE, INSTALLARE O USARE APPS CHE POSSANO RACCOGLIERE DATI AZIENDALI PRESENTI SUL CELLULARE;
- AVVERTIRE IMMEDIATAMENTE LA DIREZIONE DI OGNI EFFETTIVO O SOSPETTO AVVENIMENTO DI HACKING E/O RILEVAZIONE NON AUTORIZZATA DI DATI CONTENUTI ALL'INTERNO DEL DISPOSITIVO MOBILE.

Custodia degli strumenti di lavoro aziendali

Gli strumenti elettronici portatili non devono mai essere lasciati incustoditi.

Gli strumenti devono essere utilizzati solo ed esclusivamente per fini lavorativi e non personali e solo dalla persona autorizzata al trattamento stesso.

Istruzioni in caso di furto e di interruzione del rapporto di lavoro

Caso di furto: la persona autorizzata al trattamento deve avvisare immediatamente la Direzione (la comunicazione deve essere tempestiva per permettere la chiusura degli accessi

all'IT esterno e la cancellazione dei dati dal dispositivo mobile) e fare denuncia al più presto ai Carabinieri o alla Polizia. Copia della stessa deve essere consegnata alla Direzione.

Caso di interruzione del rapporto di lavoro: Se una persona autorizzata al trattamento cessa la sua attività deve consegnare tutti gli strumenti aziendali alla Direzione.

Utilizzo dei telefoni fissi aziendali e istruzioni da adottare durante le conversazioni telefoniche

Telefono fisso aziendale: è permesso l'utilizzo del telefono fisso aziendale a scopo personale solo per motivi d'urgenza e non sistematica; è tollerato un utilizzo personale di tale mezzo, previa autorizzazione del proprio Responsabile, solo occasionalmente e per finalità lecite (che non siano di alcun danno aziendale sia materiale che d'immagine).

Conversazioni telefoniche: In riferimento alle conversazioni telefoniche si ritiene opportuno fare presente alle persone autorizzate al trattamento quanto segue:

- DURANTE LE TELEFONATE NON È CONSENTITO FORNIRE ALCUN TIPO DI INFORMAZIONE RISERVATA O CHE IMPEGNI L'AZIENDA SULLE ATTIVITÀ SVOLTE SE NON SI È CERTI DI CHI SIA L'INTERLOCUTORE;
- NEL CASO IN CUI LA CONVERSAZIONE SIA SVOLTA IN MODALITÀ "VIVA VOCE", L'INTERLOCUTORE DEVE ESSERE INFORMATO SULL'EVENTUALE PRESENZA DI ALTRI SOGGETTI IN ASCOLTO;
- LE CONVERSAZIONI TELEFONICHE DEVONO AVVENIRE CON UN TONO DI VOCE MODERATO IN MODO TALE CHE I COLLEGHI NON VENGANO A CONOSCENZA DI INFORMAZIONI RISERVATE.

Distanza di cortesia: è obbligatorio fare rispettare e rispettare la distanza di cortesia qualora si stia dialogando con un terzo (sia collega che persona esterna) oppure si stia provvedendo alla consegna di documenti riservati.

Stampanti e Fotocopiatrici

Le stampanti e le fotocopiatrici devono essere utilizzate esclusivamente per le attività inerenti al proprio lavoro.

Non è consentito stampare o fotocopiare qualunque documento o flusso di dati di tipo personale o comunque non coerente e tanto meno in contrasto con l'attività aziendale. Non è consentito lanciare stampe dal proprio dispositivo e non ritirarle immediatamente.

Le cartelle di rete nominative.

Per lo svolgimento delle mansioni alla persona autorizzata al trattamento viene attribuita una cartella di rete nominativa aziendale. Si ricorda che la stessa deve essere utilizzata per finalità esclusivamente riconducibili allo svolgimento dell'attività lavorativa della persona autorizzata al trattamento.

Nel precisare che anche la cartella di rete è uno strumento di lavoro, si ritiene utile segnalare che:

- le informazioni ed i documenti contenuti nella cartella di rete nominativa devono essere di sola natura lavorativa e mai personale;
- la "personalizzazione" della cartella di rete non comporta la proprietà o l'usufrutto in capo alla persona autorizzata al trattamento e la liceità dell'utilizzo personale, in quanto trattasi di strumenti di esclusiva proprietà aziendale, messi a disposizione della persona autorizzata al trattamento al solo fine dello svolgimento delle proprie mansioni lavorative;
- in caso di assenza della persona autorizzata al trattamento dal posto di lavoro, l'IT potrà, in ogni momento, accedere ai dati contenuti nella cartella nominativa della persona autorizzata al trattamento assente e condividere i contenuti con il collega che svolgerà la sua mansione lavorativa in sua assenza. Tutto ciò è effettuato per consentire il normale svolgimento dell'attività lavorativa dell'azienda. La persona autorizzata al trattamento sarà tempestivamente informata e al suo rientro verranno ripristinate le impostazioni iniziali;
- l'azienda ha la facoltà di poter verificare per esigenze lavorative, anche a ritroso dopo la dimissione, il contenuto della cartella di rete nominativa, che si ricorda non essere personale e nemmeno privata;
- in caso di cessazione di attività lavorativa della persona autorizzata al trattamento, l'azienda provvederà a delegare l'accesso alla cartella di rete alla persona autorizzata al trattamento che dovrà svolgere le funzioni della persona dimessa (tale nuova persona autorizzata al trattamento riceverà opportuna nomina);
- le cartelle di rete vengono conservate per il tempo necessario anche in base ai contenuti riscontrati e all'attività svolta dall'addetto. La conservazione avvien nel rispetto dei principi

di minimizzazione, liceità, correttezza e trasparenza. Eventuali contenuti non afferenti all'attività lavorativa sono eliminati.

Utilizzo di telefoni cellulari personali per scopi personali:

L'utilizzo dei telefoni cellulari personali durante l'orario di lavoro è permesso solo per motivi urgenti. Anche in questi casi, l'utilizzo del cellulare personale non deve avvenire mentre la persona autorizzata al trattamento/lavoratore sta svolgendo la propria prestazione lavorativa. La persona autorizzata al trattamento/lavoratore disattento o comunque distratto dal telefono, può incorrere in un infortunio o esporre i colleghi a situazioni di potenziale pericolo (questa disposizione è ancora più stringente per gli addetti agli impianti, ai macchinari, ai carrelli elevatori, alla vigilanza ed al coordinamento, ecc.).

8. IL RISPETTO DELLE MISURE DI SICUREZZA INFORMATICHE

In conformità a quanto previsto dal Reg.To EU 2016/679, artt. 32 e seguenti, il Titolare, previa opportuna analisi dei rischi, ha adottato le misure tecniche ed organizzative necessarie per garantire la riservatezza, l'integrità e la disponibilità dei dati.

Il rispetto delle misure di sicurezza da parte della persona autorizzata è indispensabile e rappresenta un dovere nei confronti del Titolare. La violazione fisica o informatica di dati personali (Data breach artt. 33 e ss.) rappresenta una grave minaccia e comporta per il Titolare oneri e adempimenti, oltre che l'eventuale applicazione di sanzioni amministrative ex art. 83 punto 4 (fino a 10.000.000 di euro o 2% del fatturato aziendale) o punto 5 (fino a 20.000.000 di euro o 4% del fatturato aziendale). E' richiesta, pertanto, la massima attenzione e serietà nell'applicazione delle seguenti misure adottate:

- IL TRATTAMENTO DI DATI PERSONALI CON STRUMENTI ELETTRONICI (PC, TABLET E SMARTPHONE) È CONSENTITO SULLA BASE DI CREDENZIALI DI AUTENTICAZIONE. LE CREDENZIALI DI AUTENTICAZIONE CONSISTONO, PER I PERSONAL COMPUTER, IN UNA PASSWORD CONOSCIUTA ESCLUSIVAMENTE DALLA SINGOLA PERSONA AUTORIZZATA AL TRATTAMENTO/LAVORATORE. E' VIETATO SALVARE IN AUTOMATICO LA PASSWORD; PER GLI SMARTPHONE ED I TABLET, INVECE, IN UN PIN CONOSCIUTO ESCLUSIVAMENTE DALLA SINGOLA PERSONA AUTORIZZATA AL TRATTAMENTO/ LAVORATORE. E' VIETATO SALVARE IL PIN IN AUTOMATICO.

Le indicazioni riguardanti le modalità alle quali la persona autorizzata al trattamento deve attenersi per l'elaborazione e la scelta delle password sono le seguenti:

1. La password deve essere modificata automaticamente quando il sistema lo richiede (ogni 3 mesi). Il sistema "memorizza" le password (non sarà possibile, pertanto, riutilizzare le password precedentemente utilizzate). La persona autorizzata al trattamento dei dati personali ha, comunque, la possibilità di cambiare la password in qualsiasi momento, senza aspettare la scadenza dei mesi previsti, se questa ha perduto le qualità di segretezza adeguata.
2. Il codice per l'identificazione nominativo non può essere assegnato ad altre persone autorizzate al trattamento, neppure in tempi diversi.
3. Nel caso in cui si verifichi l'indispensabile e indifferibile necessità di accedere a trattamenti assegnati esclusivamente ad una specifica persona autorizzata al trattamento assente per un prolungato periodo e/o impossibilitato allo svolgimento delle proprie mansioni, l'IT procede a resettare la password informando tempestivamente la persona autorizzata al trattamento assente dell'intervento effettuato.
4. L'ambito del trattamento al quale la persona autorizzata al trattamento è autorizzata è definito dal profilo che gli è stato attribuito sulla base della funzione ricoperta all'interno della Azienda.
5. Nel caso di perdita, distruzione, sottrazione o altro evento che violi la segretezza delle credenziali, la persona autorizzata al trattamento deve provvedere immediatamente a notiziare la Direzione.
6. E' necessario avvertire immediatamente l'IT esterno e la Direzione di ogni effettivo o sospetto avvenimento di hacking e/o rilevazione non autorizzata di dati contenuti all'interno del dispositivo mobile. La tempestività della comunicazione consente, infatti, all'IT esterno di adottare le misure necessarie per la salvaguardia dei dati aziendali.

9. VIOLAZIONE DI DATI PERSONALI

Violazione dei dati personali (art. 4.12 - art. 33 e 34 del Regolamento Europeo 2016/679)

La violazione dei dati personali è 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".

Si intende per:

Distruzione: la distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il Titolare del trattamento

Danno: i dati personali sono stati modificati, corrotti o non sono più completi

Perdita: il caso in cui il Titolare del trattamento ha perso il controllo, l'accesso o il possesso dei dati

Trattamento non autorizzato o illecito: può includere la divulgazione di dati personali a destinatari non autorizzati oppure il trattamento di dati effettuato in violazione del regolamento.

Si indicano qui di seguito alcune situazioni esemplificative e non esaustive di possibili violazione di dati personali:

- perdita o furto di un dispositivo aziendale: perdita Chiavetta USB – Tablet - Smartphone o qualunque altro dispositivo;
- crittografia di un insieme di dati personali da parte di un ransomware (malware del riscatto);
- cancellazione accidentale di dati;
- perdita della chiave di decifratura, in caso di dati crittografati in maniera sicura;
- indisponibilità dei dati per interruzione significativa del servizio abituale dell'azienda, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (denial of service);
- accesso da persone non autorizzate ai dati personali
- comunicazione di dati a soggetti terzi non autorizzati:
  - invio di mail a persone non destinatarie del messaggio

- invio di mail in a o in cc anziché in ccn a persone terze non autorizzate (es Una e-mail di marketing diretto viene inviata ai destinatari nei campi “a” o “cc”, consentendo così a ciascun destinatario di vedere l’indirizzo e-mail di altri destinatari.)

- attacco informatico con conseguente prelievo di dati personali;

Ogni addetto designato deve comunicare immediatamente ogni accadimento alla Direzione.

10. MODALITÀ DI SVOLGIMENTO DEI CONTROLLI

Nel caso in cui un evento dannoso, fraudolento o una situazione di pericolo, non siano state evitate neppure con i preventivi accorgimenti tecnici e organizzativi sopra indicati, l’Azienda può adottare misure che consentono la verifica dei comportamenti anomali. In tal senso, gli eventuali controlli, sono eseguiti nel pieno ed assoluto rispetto di quanto previsto dalla normativa e secondo i principi di “necessità”, “correttezza” e non eccedenza. I controlli sugli strumenti di lavoro avvengono esclusivamente per ragioni organizzative, produttive, di sicurezza del lavoro e tutela del patrimonio aziendale, in conformità a quanto indicato dall’art. 4 L. 300/70.

La prima fase: controlli in forma aggregata ed anonima sulla struttura lavorativa

In prima battuta, sono effettuati solo ed esclusivamente controlli preliminari su dati aggregati riferiti all’intera struttura lavorativa. Tali controlli anonimi terminano con un avviso generalizzato all’intera struttura lavorativa in cui si è verificata l’anomalia riferendo l’utilizzo anomalo degli strumenti della società e ribadendo l’invito ad attenersi scrupolosamente ai compiti lavorativi assegnati e alle istruzioni contenute nel presente documento.

La seconda fase: controlli in forma aggregata ed anonima sulle aree

In seconda battuta, sono effettuati solo ed esclusivamente controlli preliminari su dati aggregati riferiti alle singole aree. Tali controlli anonimi terminano con un avviso generalizzato all’intera area in cui si è verificata l’anomalia riferendo l’utilizzo anomalo degli strumenti della società e ribadendo l’invito ad attenersi scrupolosamente ai compiti lavorativi assegnati e alle istruzioni contenute nel presente documento.

La terza fase: controlli individuali

Se l'utilizzo anomalo degli strumenti di lavoro aziendali, assegnati ad esclusivo uso aziendale, es: "Personal computer", "smartphone", "Tablet", "Internet", "Posta Elettronica" e "altri dispositivi", persiste, si procede ad effettuare controlli sull'operato della singola persona autorizzata al trattamento, nel rispetto della massima riservatezza e da personale appositamente autorizzato e formato dal Titolare del trattamento.

In caso di violazioni informatiche di rilievo, l'IT esterno, debitamente coinvolto, può procedere, in ogni momento, ad un controllo individuale immediato attraverso gli strumenti di controllo adottati dall'Azienda (es: log di sistema navigazione, ecc…) in relazione al dispositivo interessato e al soggetto a cui è attribuito (o che in quel momento lo sta utilizzando). L'urgenza della tutela del patrimonio aziendale, di conseguenza anche dei dati, può giustificare il mancato rispetto delle fasi precedentemente segnalate (Fase 1 e Fase 2).

Conseguenze a livello giuridico e disciplinare

In relazione a quanto previsto dall'art. 4 L. 300/70, i dati acquisiti con i controlli effettuati possono essere utilizzati per tutti i fini connessi al rapporto di lavoro, inclusi eventuali richiami disciplinari e quanto previsto dalla normativa del lavoro applicabile.

L'Azienda verifica, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità aziendali (Pc portatile o fisso, smartphone, Tablet, internet, casella di posta elettronica, rete aziendale ecc....). In caso di illecito l'Azienda, pur nel pieno e costante rispetto della normativa del Regolamento Europeo a tutela del lavoratore, si riserva di segnalare (per obbligo di legge, per tutela propria, dei colleghi di lavoro e dei terzi in genere) alle competenti Autorità comportamenti costituenti reato e condanne penali. Si riserva, altresì, di agire sotto il profilo civilistico/amministrativo/disciplinare in caso di mancato rispetto delle presenti istruzioni, o in presenza di altri tipi di violazione.

11. TRATTAMENTO SENZA STRUMENTI ELETTRONICI (DOCUMENTI CARTACEI)

Anche per quanto riguarda il trattamento dei documenti cartacei, la persona autorizzata al trattamento deve rispettare le indicazioni del Titolare del trattamento e dei referenti interni alla gestione della privacy in merito agli archivi a cui poter accedere e ai documenti da trattare.

Con queste premesse e con l'obiettivo di assicurare la massima riservatezza, vengono rilasciate le seguenti istruzioni operative:

- l'Azienda ha predisposto luoghi appositi (armadi e cassettiere) dove conservare i documenti contenenti dati personali; questi vengono comunicati all'occorrenza, come pure eventuali variazioni degli stessi. Come regola generale, tali documenti non devono essere rimossi se non per effettuare le operazioni di trattamento e solo per il tempo necessario. Al termine dell'elaborazione i documenti riservati devono essere riposti nella posizione designata. I documenti riservati e/o che contengono dati sulla salute e/o particolari e/o relativi a condanne penale e reati non devono essere lasciati sulle scrivanie.
- gli atti e i documenti, una volta presi in carico, contenenti dati personali, non devono essere lasciati liberi di vagare senza controllo ed a tempo indefinito negli uffici, ma occorre controllarli e custodirli, per poi restituirli al termine delle operazioni affidate;
- in caso di affidamento di atti e documenti contenenti dati sulla salute, particolari o relativi a condanne penale e reati, il controllo e la custodia devono avvenire in modo tale che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario che gli uffici, gli armadi e le cassettiere, ovunque si trovino, siano chiusi con serratura o con altri accorgimenti aventi funzione equivalente;
- accertarsi che un visitatore o un terzo (o collega autorizzato o non che si intrattiene per troppo tempo) non entri in ufficio e venga a conoscenza dei contenuti dei documenti;
- limitare al minimo il numero di fotocopie effettuate (solo se veramente necessario e non in modo ridondante). Tali documenti devono essere gestiti con le stesse identiche procedure previste per l'originale;
- i documenti contenenti dati personali non più necessari o inutilizzati non devono essere semplicemente cestinati, ma fisicamente resi inutilizzabili da chiunque (es. è vietato cestinare fogli interi o parte di foglio che siano compiutamente leggibili),
- se i documenti devono essere portati all'esterno del luogo del lavoro, bisogna evitare che soggetti non autorizzati ne possano prendere visione (contenitore chiuso – es busta sigillata);

- evitare assolutamente di discutere e/o comunicare dati personali per telefono se non si è sufficientemente certi che il corrispondente sia a sua volta autorizzato a venirne a conoscenza;
- evitare di lasciare incustoditi, o peggio dimenticare, documenti contenenti dati personali nella fotocopiatrice, sul fax, nella stampante, (ecc…);
- non sottrarre, cancellare, distruggere senza autorizzazione dati, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- non consegnare a persone non autorizzate stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.

12. LINEE GUIDA PER I DIPENDENTI SUI SOCIAL MEDIA

(istruzioni valide sia per le persone autorizzate al trattamento sia per i lavoratori che utilizzano gli strumenti aziendali ma che non hanno ricevuto la nomina come persona autorizzata al trattamento)

Per Social Media si intende qualunque sito Web nel quale le persone autorizzate al trattamento dei dati personali/lavoratori sono in grado di condividere contenuti con molti altri visitatori. I contenuti condivisi possono includere informazioni personali, opinioni, commenti, video, foto, informazioni commerciali, ecc. Esempi di tali applicazioni web sono: Facebook, Twitter, YouTube, LinkedIn…. Anche blog, forum e community sono considerati Social Media.
Si ritiene opportuno ricordare alle persone autorizzate al trattamento/lavoratori che la riservatezza deve essere rispettata anche nell'utilizzo personale dei social media in quanto anche l'uso personale dei social media da parte delle persone autorizzate al trattamento/lavoratori, al di fuori delle proprie mansioni, può arrecare danno all'immagine della Azienda.

Le persone autorizzate al trattamento/lavoratori sono responsabili dei contenuti che pubblicano nei Social Media e ne rispondono ai sensi di legge, in sede civile, penale, amministrativa e disciplinare. Si ricorda che il diritto di critica nei confronti del datore di lavoro (Azienda), sia esso esercitato sui Social Media come in qualsiasi altro contesto pubblico, è soggetto a stringenti limiti di veridicità dei fatti e continenza sostanziale e formale. Qualsiasi

dichiarazione che comporti una lesione del decoro aziendale con eventuale danno d'immagine e relativo danno economico, rappresenta un comportamento idoneo a ledere la fiducia alla base del rapporto di lavoro, con violazione del dovere previsto dall'art. 2015 C.C... Tale predetto comportamento può avere rilievo disciplinare e, nei casi più gravi, costituire presupposto per giusta causa di licenziamento. Qualsiasi comunicazione, pertanto, deve rispettare la politica e l'immagine aziendale.

La circolazione delle informazioni inserite nei social media, non è contenibile, né governabile dall'autore. La pubblicazione di dati sui Social Media è configurabile come operazione di diffusione del dato ai sensi del Regolamento Europeo 2016/679 e pertanto soggetta alla speciale disciplina restrittiva prevista dal Regolamento stesso.

Si ricorda di attenersi alle seguenti istruzioni:

a) attenersi alle norme del Regolamento Europeo 2016/679 e alle indicazioni fornite dall'Azienda;

b) attenersi alle norme in tema di copyright e riservatezza aziendale;

c) evitare di pubblicare contenuti lesivi per l'immagine dell'Azienda;

d) evitare di divulgare o utilizzare informazioni di qualsiasi natura relative all'Azienda ed al proprio lavoro svolto per l'Azienda;

e) evitare di divulgare o utilizzare foto e/o immagini scattate all'interno dell'Azienda;

f) informare il vostro responsabile (soprattutto in caso di dubbi) sui contenuti che si desidera pubblicare on-line in relazione all''attività dell'Azienda.

I social media sono paragonabili ad un qualunque contesto sociale - una riunione, una festa, quattro chiacchiere al bar. E' necessario, quindi, fare in modo che le azioni e i comportamenti sui social media siano in linea con l'immagine che si desidera trasmettere di sé sul posto di lavoro.

L'Azienda, nel caso di pubblicazione di contenuti inappropriati o riservati, si riserva di intervenire in qualsiasi sede con le relative conseguenze.

13. MODALITÀ PER ELABORARE E CUSTODIRE LE PASSWORD

Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione.

Se si è in possesso di più credenziali di autenticazione, è opportuno accedere ai dati unicamente con la credenziale relativa al trattamento in oggetto.

Rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria Nomina ad Addetto.

Elaborare le password seguendo le istruzioni sotto riportate.

SCELTA DELLE PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

- NON comunicare a nessuno la password (lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare dati e risorse di utilizzo personale)
- NON scrivere la password in nessun posto in cui che possa essere letta facilmente, soprattutto vicino al computer.
- NON scegliere password che si possono trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per appurare quale sia quella giusta.
- NON usare il nome utente come password.
- NON usare password come il proprio nome o quello della moglie/marito, figli, cane, date di nascita, numeri di telefono etc.

COSA FARE OBBLIGATORIAMENTE

- la password deve essere composta da almeno otto caratteri o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica;

- l'Addetto deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema;
- la password deve essere modificata dall'Addetto ogni volta che il sistema lo richiede o l'utente lo ritenga necessario per una maggiore sicurezza e riservatezza;

COSA FARE PRATICAMENTE

Utilizzare più di una parola e creare password lunghe

A volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata, e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare.

E' bene sapere che diversi strumenti di intercettazione presumono che le password non siano formate da più di 14 caratteri, le password molto lunghe (da 14 a 128 caratteri), pertanto, possono rappresentare un'ottima protezione contro possibili violazioni. Non tutti i software sono tuttavia in grado di accettare password superiori a 14 caratteri: ad esempio i sistemi operativi Windows 95 98 non oltrepassano questo limite.

Utilizzare numeri e simboli al posto di caratteri

E' opportuno non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:

- Caratteri minuscoli: a, b, c,...
- Caratteri maiuscoli: A, B, C,...
- Caratteri numerici: 0,1,2,3,4,5,6,7,8,9
- Caratteri non alfanumerici: (< > , .) ` ~ ! $ % ^ ; * - + = | \ { @ # } [/] : ; " '?

E' preferibile non inserirli alla fine di una parola nota come ad es.:"computer987". In questo caso la password, infatti, può essere identificata abbastanza facilmente. Al contrario, è sufficiente sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente. Ad esempio si può provare a utilizzare "@"al posto di "A", "$"al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3"al posto di "E": si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri. Con

alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio (es.: "Ve$tit0 di Mari0"), già sufficientemente lunghe e estremamente difficili da identificare o decifrare.

13. AGGIORNAMENTI PERIODICI

Il presente documento è soggetto ad aggiornato periodico in funzione degli aggiornamenti normativi e dell'evoluzione tecnologica. E' indispensabile, pertanto, fare riferimento sempre all'ultima versione.

14. REFERENTI AZIENDALI

In caso di dubbi, esigenze pratiche ed operative, per supporto tecnico hardware e software, su quanto sopra esposto è necessario rivolgersi al seguente indirizzo email privacy@lazzarospallanzani.it e/o ai referenti interni della gestione della privacy.