MODELLO ORGANIZZATIVO PRIVACY

Azienda/Organizzazione	**Ordine dei Periti Industriali delle Province di Ancona e Macerata**

SEDE	SEDE LEGALE E OPERATIVA VIA ACHILLE GRANDI 14/E 60027 OSIMO - AN

Data redazione: 16/09/2021

Il presente manuale intende rappresentare una guida in materia del trattamento dei dati personali di persone fisiche adottato da Ordine dei Periti Industriali delle Province di Ancona e Macerata

DATI ORDINE

Ragione Sociale	**Ordine dei Periti Industriali delle Province di Ancona e Macerata**
Partita IVA	- / CF 80007810429
Codice fiscale	80007810429
Sede legale	VIA ACHILLE GRANDI 14/E, 60027 OSIMO - AN
Contatti	071.7108118 – segreteria@periti-industriali.an.it
Sito web	www.periti-industriali.an.it
Attività economica	Ordine professionale
Codici ATECO	• 94.99.90 - Attività di altre organizzazioni associative nca
Rappresentante legale	BALLARINI RENZO
Codice fiscale	BLLRNZ57D23A271V
Contatti	

SEDI

Denominazione	**SEDE LEGALE E OPERATIVA**
Tipo	- Legale - Amministrativa - Operativa
Indirizzo	VIA ACHILLE GRANDI 14/E, 60027 OSIMO - AN

General Data Protection Regulation (GDPR)

1. L'ADEGUAMENTO DELLA NORMATIVA NAZIONALE

Il Regolamento UE n. 2016/679, General Data Protection Regulation (di seguito anche "Regolamento" o "GDPR") è un atto di diritto dell'Unione Europea attraverso il quale la Commissione Europea intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione Europea (UE).

Il nuovo Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, entrato in vigore il 24 maggio 2016 e direttamente applicabile all'interno degli Stati membri dal 25 maggio 2018, introduce una serie di obblighi finalizzati a garantire lo svolgimento di lecite e corrette operazioni di trattamento di dati personali da parte delle organizzazioni, in qualità di Titolari e/o Responsabili del trattamento.

In Italia il processo di adeguamento al GDPR è stato condotto attraverso l'adozione del Decreto Legislativo 10 agosto 2018, n. 101, in vigore dal 19 settembre 2018, il quale è intervenuto sul preesistente D.lgs. 196/2003 – c.d. Codice Privacy - mediante congiunti interventi integrativi, modificativi e di abrogazione.

Il Regolamento si applica ai dati dei residenti nell'Unione Europea e anche a imprese ed enti, organizzazioni in generale, con sede legale fuori dall'UE che trattano dati personali di residenti nell'Unione Europea. Si precisa pertanto che devono adeguarsi alla normativa tutte le imprese, le organizzazioni e le Pubbliche Amministrazioni presenti negli stati membri dell'Unione Europea (indipendentemente dal fatto che il trattamento sia effettuato in UE), ma anche società extra UE che offrono servizi o prodotti a persone fisiche nel territorio dell'UE o che semplicemente monitorano il comportamento di soggetti all'interno dell'Unione.

L'adeguamento ai requisiti previsti dal GDPR comprende, tra le altre attività di privacy compliance, l'adozione e l'efficace ed effettiva attuazione di un "Modello Organizzativo in Materia di Protezione dei Dati Personali" (di seguito anche "Modello Organizzativo Privacy" o "MOP") che consenta alle imprese, enti ed organizzazioni, cui si applica il Regolamento, di:

(i) predisporre un sistema di controllo idoneo a prevenire i rischi privacy relativi ai dati personali, come sopra identificati e successivamente valutare i controlli esistenti, in termini di adeguatezza ai requisiti previsti dal GDPR ed effettiva operatività degli stessi;
(ii) gestire tempestivamente possibili criticità;
(iii) dare evidenza del sistema di controllo implementato evitando l'imputazione di responsabilità e delle sanzioni previste.

2. I PRINCIPI GENERALI E LE NUOVE REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali deve essere effettuato nel rispetto dei seguenti principi generali:

- **il diritto alla protezione del dato personale**, secondo il quale ogni individuo ha il diritto che il

trattamento dei suoi dati personali avvenga, secondo modalità che assicurino un elevato livello di tutela, nel rispetto dei suoi diritti e libertà fondamentali, nonché della sua dignità, conparticolare riferimento alla riservatezza e all'identità personale;

- **il principio di liceità e correttezza**, che prescrive al soggetto che agisce sui dati personali la conformità alla legge del trattamento posto in essere e la trasparenza per l'interessato della raccolta e delle altre operazioni, vietando artifizi e raggiri. I dati personali trattati in violazione della normativa in materia protezione dei dati personali non possono essere utilizzati;

- **il principio di finalità**, secondo cui la raccolta dei dati deve essere collegata alla finalità perseguita, che deve essere legittima, determinata e non incompatibile con l'impiego dei dati;

- **il principio di necessità nel trattamento dei dati e di minimizzazione del loro utilizzo**, che impone che la raccolta e il trattamento di dati vada effettuato limitatamente alle sole informazioni necessarie all'attività, in modo da ridurre al minimo l'utilizzo di dati personali e di dati identificativi. Infatti, laddove le stesse finalità possano essere perseguiteanche senza l'uso di dati personali, il trattamento deve riguardare solo dati anonimi oppure deve essere posto in essere adottando opportune modalità che permettano di identificare l'interessato solo in caso di necessità;

- **il principio di proporzionalità**, che prevede altresì di verificare, in ogni fase del trattamento,se le singole operazioni siano in concreto pertinenti e non eccedenti le finalità perseguite;

- **il principio di tutela dell'integrità del dato**, secondo il quale i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di adeguate misure tecniche ed organizzative, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- **il principio di Accountability o di responsabilizzazione**, sulla base del quale tutti i dati devono essere trattati dal Titolare in modo responsabilizzato. Il Titolare deve quindi dimostrare, per ciascun trattamento, di aver agito in conformità alle disposizioni del GDPR. **L'approccio metodologico da applicarsi al fine di garantire l'Accountability è un approccio "risk based"**, ovvero l'approccio basato sulla valutazione del rischio del trattamento, che deve essere adottato e dimostrato da parte delle imprese, enti, o organizzazioni è di tipo proattivo, e non più reattivo, con focus su obblighi e comportamenti finalizzati a prevenire in modo effettivo il possibile evento di danno. Il rischio inerente al trattamento è da intendersi come rischio per la sicurezza dei dati e come rischio di impatti negativi sulle libertà e i diritti degli interessati. Tali impatti devono essere analizzati attraverso un apposito processo di valutazione (es. Risk e Privacy Impact Assessment) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) da adottare per mitigare tali rischi. L'approccio metodologico "risk based" deve quindi seguire logiche di risk assessment e risk management, al fine di valutare e ridurre il rischio per i diritti e le libertà dei soggetti dei dati e individuare le misure tecniche e organizzative idonee a garantire un adeguato livello di sicurezza;
- **Privacy by Design**, che sottende la necessità di prevedere, già in fase di progettazione del

trattamento dati e dei sistemi informatici e applicativi, l'adozione di logiche di minimizzazione del trattamento e di disegno dello stesso sin dall'origine in linea coi principi in esame. Ogni titolare deve quindi assicurare che i sistemi informatici, prodotti e/o servizi offerti che prevedono il trattamento di dati personali nonché ogni progetto avviato siano, per impostazione predefinita, protetti da adeguate misure di sicurezza e garantiscano il più ampio rispetto dei diritti e delle libertà degli interessati in ottemperanza alla normativa inmateria di protezione dei dati personali, senza che sia richiesto a questi ultimi alcun ulteriore intervento;

- **Privacy by Default** che implica l'implementazione da parte dell'organizzazione di un processo che preveda e disciplini le modalità di acquisizione, trattamento, protezione e modalità di diffusione dei dati personali, limitando la raccolta dei dati esclusivamente aquei dati personali realmente necessari per la realizzazione delle finalità perseguite, in ottemperanza al principio di minimizzazione dei dati, e determinando sin dall'origineil periodo per il quale i dati personali raccolti dovranno essere conservati;

- **Consenso**, che deve essere esplicitamente prestato per ogni trattamento effettuato, ove non operino le esenzioni di legge. A tal proposito, se la richiesta per ottenere il consenso dagli interessati viene inserita nell'ambito di altre dichiarazioni essa va distinta e formulata con linguaggio semplice e chiaro. Condizione di validità del consenso è che le finalità per cui viene richiesto siano esplicite, legittime, adeguate e pertinenti. Nel caso in cui il consenso altrattamento dei dati personali per una o più specifiche finalità riguardi i minori, il GDPR richiede al Titolare del trattamento la verifica documentata dell'età del minore e, laddove necessario sulla base dell'età del minore, del consenso al trattamento da parte di un genitoreo da chi eserciti la responsabilità genitoriale. I Titolari del trattamento dei dati devono essere in grado di dimostrare che l'interessato abbia prestato il consenso (i.e. principio "opt-in") e ilconsenso possa essere ritirato o modificato;

- **Data Breach**, definito come qualsiasi attività che comporti la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattatati. Nei casi di violazione dei dati, accesso abusivo o, comunque, perdita degli stessi, i Titolari dei trattamenti saranno obbligati, entro 72 ore, ad avvisare l'Autorità di Controllo e, nei casi di particolare gravità, anche i diretti interessati, informando in relazione alle possibili conseguenze, alle misure adottate per rimediare o ridurre l'impatto del danno e ai dati di contatto degli organi e delle figure aziendali che vigilano sulla gestione e protezione del trattamento di dati personali in conformità alla legge;

- **Diritti degli interessati**, che includono tra l'altro: (i) diritto di accesso, che prevede il diritto di accedere e/o richiedere quali dati personali siano oggetto di trattamento con indicazione, ad esempio, del periodo di conservazione previsto o i criteri per definire tale periodo, nonché delle garanzie applicate in caso di trasferimento dei dati verso Paesi terzi; (ii) diritto alla cancellazione (diritto all'oblio), che prevede il diritto dell'interessato alla cancellazione dei propri dati personali ove non sussistano obblighi di legge o interessi prevalenti del Titolare; nonché l'obbligo per il Titolare o il Responsabile del trattamento di informare della richiesta di cancellazione altri Titolari che trattano i dati personali da cancellare, dando comunicazione all'interessato, dietro richiesta del medesimo, dei destinatari a cui ha trasmesso la sua richiesta di cancellazione; (iii) diritto di limitazione, che prevede, in caso di violazione dei presupposti di liceità del

trattamento, la richiesta di limitazione del trattamento, in attesa della valutazione del Titolare, o di richiesta di rettifica dei dati presentata dall'interessato; (iv) diritto alla portabilità dei dati, che si applica ai soli dati automatizzati trattati con il consenso dell'interessato o sulla base di un contratto con lo stesso e forniti al Titolare dall'interessato medesimo, nei casi in cui lo stesso abbia la necessità di trasferirli ad un altro Titolare, laddove tecnicamente possibile;

- **Trasferimento dati extra UE**: Il GDPR vieta il trasferimento verso Paesi situati al di fuori dell'UE o organizzazioni internazionali se effettuato in assenza di adeguati standard di tutela. Al contrario, invece, è permesso in caso di presenza di adeguate garanzie come clausole contrattuali tra Titolari autorizzate dal Garante, accordi e provvedimenti vincolanti tra autorità pubbliche amministrative e giudiziarie, clausole tipo adottate dal Garante, adesione a codici di condotta e/o meccanismi di certificazione. È inoltre permesso il trasferimento oltre UE in caso di decisioni di adeguatezza della Commissione UE (es. «Privacy Shield EU/USA», Svizzera, Argentina, Australia, Canada, ecc.), norme vincolanti di impresa (Binding Corporate Rules – «BCR») e casi in deroga (consenso informato dell'interessato, necessità per esecuzione adempimenti contrattuali e precontrattuali, interesse pubblico, diritto di difesa, interessi vitali, dati tratti da registro pubblico, ecc.);

- **Data Protection Officer**, definito ai sensi del Regolamento come il Responsabile della Protezione dei dati personali o Data Protection Officer (DPO) che deve essere designato per fornire una consulenza ed assistenza giuridica e tecnica specialistica sulle questioni afferenti alla data protection. Con riguardo all'attribuzione degli specifici compiti contemplati dal Regolamento, il DPO deve avere una serie di requisiti (a titolo esemplificativo, competenze giuridiche, competenze tecniche e di security) che consentano allo stesso di operare un risk assessement, ovvero valutare i rischi e fornire pareri su temi IT/Security ai fini dell'applicazione delle soluzioni e delle misure informatiche di sicurezza più adeguate. Svolge un ruolo di attivatore e, a suo carico, può rinvenirsi un dovere di impulso anche rispetto al Titolare e al Responsabile del trattamento che rimanga inattivo, violando il Regolamento. Secondo quanto previsto dell'art. 39 del GDPR, il DPO è autorizzato ad attribuire le responsabilità, sensibilizzare e formare il personale aziendale e chiunque sia coinvolto nelle attività di gestione dei trattamenti dei dati e nelle connesse attività di controllo, stabilendo chi e in quale misura, all'interno dell'impresa, ente o organizzazione, deve rispondere di eventuali comportamenti non conformi alle procedure interne di gestione dei dati. Il DPO supporta il Titolare nella tenuta del Registro dei trattamenti e fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati, sorvegliandone lo svolgimento ai sensi dell'articolo 35 del GDPR. Coopera, inoltre, con l'Autorità di controllo e funge da punto di contatto con la medesima per questioni connesse al trattamento dei dati;

- **Misure tecniche ed organizzative adeguate**, tra cui Informative, nomine, formazione ecc. e soprattutto procedure interne che formalizzino nell'ambito delle stesse adeguati controlli imposti dal GDPR e della concreta realizzazione di un sistema di compliance adeguato ad evitare un trattamento illecito dei dati personali e in grado di dimostrare che l'organizzazione aziendale ha proattivamente adottato e attuato tutti i presidi previsti dal Regolamento.

3. RESPONSABILITA'

Il trattamento dei dati personali in violazione della normativa può dare luogo ad una responsabilità di carattere civile e/o penale e/o amministrativa, ovvero anche cumulativa in relazione ad un fatto unico.

In ambito civile, può legittimare una richiesta al risarcimento per danni da parte del soggetto leso, come previsto dal Codice civile ed in particolare dall'art. 2050 c.c., secondo il quale chiunque, sia esso persona fisica o persona giuridica, cagiona un danno ad altri per effetto del trattamento di dati personali e non dimostri di aver adottato misure idonee ad evitarlo, è tenuto al risarcimento del danno medesimo.

La responsabilità legata al trattamento dei dati personali rientra infatti nel concetto di responsabilità per esercizio di attività pericolose, secondo il quale - ai sensi dell'art. 2050 c.c. sopra richiamato - "chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati è tenuto al risarcimento se non prova di avere adottato tutte le misure idonee ad evitare il danno".

Il concetto di responsabilità sopra definito, già contemplato dalla normativa in materia di privacy, si configura a prescindere dal comportamento colposo o doloso dell'autore, il quale, in virtù di un'inversione dell'onere della prova, per esimersi dalla responsabilità a suo carico, deve dare la dimostrazione di una prova liberatoria, ovvero di avere adottato tutte le misure atte ad evitare il danno avvenuto. Spetta a colui che ha subito il danno fornire la prova del danno medesimo e la dimostrazione del rapporto di causalità tra l'attività pericolosa esercitata ed il danno. I danni risarcibili possono essere di natura sia patrimoniale che non patrimoniale, intendendosi in quest'ultimo caso quei danni, liquidati in via equitativa da parte del giudice, derivanti dalla sofferenza fisica e/o morale del danneggiato.

Con riguardo alla responsabilità penale, le fattispecie criminose che assumono maggior rilevo riguardano il reato di accesso abusivo ad un sistema informatico o telematico (art. 615 ter Codice Penale), il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater Codice Penale), nonché i reati previsti dal D.lgs. 196/2003 Codice in materia di protezione dei dati personali – c.d. Codice Privacy – come modificato dal D.lgs. 101/2018, e in particolare l'art. 167 - Trattamento illecito di dati, l'art. 167 bis - Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala, l'art. 167 ter - Acquisizione fraudolentadi dati personali oggetto di trattamento su larga scala, l'art. 168 - Falsità nelle dichiarazioni e notificazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante, l'art. 170 - Inosservanza di provvedimenti del Garante e l'art. 171 - Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.

Con riguardo, infine, alla responsabilità amministrativa, il Regolamento stabilisce sanzioni amministrative che vanno inflitte, in funzione delle circostanze di ogni singolo caso, tenendo in debito conto i seguenti elementi: a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; b) il carattere doloso o colposo della violazione; c) le misure adottate dal Titolare del trattamento o dal Responsabile del trattamento perattenuare il danno subito dagli interessati; d) il grado di responsabilità del Titolare del trattamento odel Responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messein atto; e) eventuali precedenti violazioni pertinenti commesse dal Titolare del trattamento o dal Responsabile del

trattamento; f) il grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) le categorie di dati personali interessate dalla violazione; h) la maniera in cui l'Autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il Titolare del trattamento o il Responsabile del trattamento ha notificato la violazione; i) il rispetto di tali provvedimenti; j) l'adesione ai codici di condotta o ai meccanismi di certificazione; e k) eventuali altri fattori aggravanti o attenuanti applicabilialle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

In caso di violazioni della normativa in vigore sono passibili di responsabilità e quindi tenuti al risarcimento il Titolare del trattamento ed il Responsabile del trattamento. Il Titolare deve risarcire qualsiasi danno a lui imputabile che abbia cagionato a causa della violazione del Regolamento nel trattamento dei dati.

Il Responsabile risponde dei danni a lui imputabili se non ha adempiuto agli obblighi a lui specificatamente diretti o ha agito in modo difforme o contrario alle istruzioni del Titolare.

4. SANZIONI

L'art. 82 del GDPR disciplina il diritto al risarcimento e responsabilità in forza del quale chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento.

Il sistema sanzionatorio prevede, a fronte del compimento di violazioni del Regolamento, in funzione delle circostanze di ogni singolo caso, l'applicazione delle seguenti sanzioni amministrative pecuniarie:

- una multa fino a 10 milioni di euro o, se superiore, fino al 2% del volume d'affari globale registrato nell'anno precedente, nei casi previsti dall'articolo 83, paragrafo 4 del Regolamento (a titolo esemplificativo, in caso di: mancata adozione delle tutele per i minori, sui dati anonimizzati, delle misure privacy by design e by default, contitolari, registri del trattamento, privacy impact assessment, istruzioni agli autorizzati, misure di sicurezza, data protection officer);
- una multa fino a 20 milioni di euro o, se superiore, fino al 4% del volume d'affari globale registrato nell'anno precedente, nei casi previsti dall'articolo 83, paragrafi 5 e 6 del Regolamento (a titolo esemplificativo, in caso di mancato rispetto dei principi di base del trattamento, dei diritti degli interessati, delle regole sui trasferimenti di dati extra UE, ecc.).

Nell'ambito del GDPR viene stabilito un margine di discrezionalità circa la possibilità di infliggere una sanzione e la determinazione dell'importo della stessa. Ciò non implica un'autonomia gestionale delle sanzioni in capo alle Autorità nazionali competenti, ma fornisce, a queste ultime, alcuni criteri su come interpretare le singole circostanze del caso. I criteri per la determinazione delle sanzioni amministrative pecuniarie (come, a titolo esemplificativo, la natura, gravità e durata della violazione,il carattere doloso o colposo della violazione, il grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi) sono stabiliti all'articolo 83 paragrafo 2 del Regolamento.

In sede di adeguamento nazionale alle disposizioni del GDPR, il D.lgs. 196/2003, come modificato dal

D.lgs. 101/2018, all'art. 166 ha fornito ulteriori indicazioni in relazione ai criteri di applicazione delle sanzioni amministrative pecuniarie e in relazione al procedimento per l'adozione dei provvedimenti correttivi e sanzionatori.

È offerta all'Autorità nazionale l'opportunità di sostituire la sanzione pecuniaria con un ammonimento, "in caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica" (cfr. Considerando 148).

Secondo quanto stabilito dal Considerando 149 e dall'art. 84 del GDPR, l'Italia ha introdotto disposizioni relative a sanzioni penali come strumento di attuazione e tutela della nuova disciplina. In particolare, il D.lgs. 196/2003, come modificato dal D.lgs. 101/2018, ha previsto specifiche fattispecie penali agli artt. 167, 167 bis, 167 ter, 168, 170 e 171.

Secondo l'articolo 58 del GDPR, le Autorità possono avvalersi inoltre di una serie di poteri correttivi come la possibilità di limitare o addirittura vietare un trattamento dei dati da parte dell'azienda. Tutto ciò potrebbe portare l'organizzazione ad un'interruzione di un servizio o un'attività aziendale.

5. IL MODELLO ORGANIZZATIVO PRIVACY DELL'ORDINE DEI PERITI INDUSTRIALI DELLE PROVINCE DI ANCONA E MACERATA

5.1 FINALITA' DEL MODELLO ORGANIZZATIVO PRIVACY

Il presente documento costituisce il Modello Organizzativo Privacy dell' Ordine dei Periti Industriali delle Province di Ancona e Macerata (di seguito "Ordine"), che effettua trattamenti di dati personali, nella sua qualità di Titolare e/o di Responsabile.

Tale documento descrive le attività poste in essere dall'Ordine per assicurare la conformità al GDPR e il relativo approccio metodologico utilizzato, oltre agli aspetti di governance, risk management e compliance applicabili alla protezione dei dati personali con la finalità di definire:

i. i meccanismi organizzativi e gestionali, inclusi ruoli, responsabilità in materia di protezione dei dati personali ("governance");
ii. le modalità di gestione dei rischi in materia di protezione dei dati personali ("risk management");
iii. un sistema strutturato di procedure a presidio dei rischi che sono stati rilevati, nonché una costante azione di monitoraggio sulla corretta attuazione di tale sistema in conformità ai requisiti normativi applicabili in materia di protezione dei dati personali ("compliance").

L'Ordine, consapevole dell'importanza di adottare ed efficacemente attuare un Modello Organizzativo Privacy, ha predisposto questo documento, che costituisce un valido strumento di sensibilizzazione dei destinatari (come definiti al paragrafo 5.1) per assumere comportamenti conformi ai requisiti del GDPR.

5.2 DESTINATARI

Le disposizioni del presente Modello Organizzativo Privacy sono vincolanti per i dipendenti (ivi inclusi i dirigenti), per i collaboratori sottoposti a direzione o vigilanza dell'Ordine e per tutti coloro che, pur non appartenendo all'Ordine, operano a vario titolo gestendo attività che implicano il trattamento di dati personali (di seguito i "Destinatari").

5.3 ELEMENTI FONDAMENTALI DEL MODELLO ORGANIZZATIVO PRIVACY

Gli elementi fondamentali del Modello Organizzativo Privacy, sviluppati dall'Ordine nell'ambito delle attività di adeguamento al GDPR, possono essere così riassunti:

- la predisposizione e l'adozione di una Procedura per la gestione del Data Breach;
- la redazione di istruzioni per la gestione della documentazione aziendale;
- l'aggiornamento della documentazione privacy rilevante (es. informative, consensi, nomine interne ed esterne);
- l'adozione e l'aggiornamento del Registro dei trattamenti;
- la programmazione di attività di informazione e formazione sui contenuti e i cambiamenti introdotti dal GDPR e volte alla diffusione del presente Modello Organizzativo Privacy;
- la previsione di implementazione di attività periodiche di verifica, anche a campione, per il monitoraggio sull'adeguata attuazione del GDPR, sull'efficacia ed effettiva operatività del Modello Organizzativo Privacy, anche ai fini del riesame dello stesso, e del sistema delle procedure adottate.

5.4 RIFERIMENTI NORMATIVI

Il presente documento fa riferimento e si ispira alle seguenti norme:

- "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
- Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- Standard UNI EN ISO / IEC 27001:2013 "Tecnologia per l'Informazione – Tecniche per la Sicurezza – Sistemi di Gestione per la Sicurezza delle Informazioni – Requisiti";
- Linee Guida e Provvedimenti specifici dell'Autorità Garante per la Protezione dei Dati Personali;
- ARTICLE 29 DATA PROTECTION WORKING PARTY: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

6. TERMNI E DEFINIZIONI

GDPR

General Data Protection Regulation (Regolamento Europeo UE 2016/679).

Trattamento
Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Dato personale
Qualsiasi informazione concernente una persona fisica identificata o identificabile (art. 4 GDPR), anche indirettamente, oppure informazioni (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari.

Dati particolari
I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Profilazione
Per profilazione si intende l'insieme delle attività di raccolta ed elaborazione dei dati inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento. In ambito commerciale, la profilazione dell'utente è il mezzo che consente la fornitura di servizi personalizzati oppure l'invio di pubblicità comportamentale.

Pubblicità comportamentale
La pubblicità comportamentale è una tecnica basata sul tracciamento (tracking) delle attività online degli utenti, al fine di costruire dei profili degli utenti con lo scopo di offrire loro pubblicità più rilevante per gli utenti stessi, e quindi più efficace.

Titolare
Il Titolare del trattamento (data controller) 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" (art. 4. par. 1, n. 7 GDPR).

Responsabile del trattamento
Il responsabile del trattamento è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare (art. 4, par. 1, n. 8 GDPR).

Sub responsabile
Il responsabile del trattamento può nominare responsabili di secondo livello a meno che non sia vietato dalle istruzioni del titolare. È comunque il responsabile principale a rispondere di fronte al titolare del trattamento dell'operato dei sub-responsabili. Al sub-responsabile devono essere fornite le istruzioni e deve operare nel rispetto degli obblighi imposti al responsabile del trattamento.

Persona autorizzata
Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato
La persona fisica a cui si riferiscono i dati personali.

Banca dati
Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Misure di sicurezza
Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che assicurano un livello di protezione adeguato dei dati personali.

Strumenti elettronici
Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica
L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione
I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Parola chiave/Password
Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione
L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione
L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

7. RUOLI, COMPITI E NOMINA DEI SOGGETTI

7.1 Titolare del Trattamento
Il **Titolare del trattamento è** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Responsabili del trattamento dati** che assicurino e garantiscano che vengano adottate le misure di sicurezza. Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile del trattamento dei dati** ne assumerà tutte le responsabilità e

funzioni.

7.2 Responsabile del Trattamento dati

Il responsabile del trattamento (data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR).
Si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.
Il titolare del trattamento risponde della gestione effettuata dal responsabile, dovendo ricorrere a responsabili che presentino garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che soddisfino i requisiti del Regolamento (Considerando 81 GDPR), e che le sue decisioni siano conformi alle leggi. Compito specifico del titolare è, infatti, quello di valutare il rischio del trattamento che pone in essere tramite i responsabili. Il titolare deve sempre poter sindacare le decisioni dei responsabili.
Il responsabile ha obblighi di trasparenza, occorre, infatti contrattualizzare il rapporto tra titolare e responsabile specificando gli obblighi ed i limiti del trattamento dati. Il responsabile riceverà, tramite atto giuridico (cioè per iscritto), tutte le istruzioni in merito ai trattamenti operati per conto del titolare, alle quali dovrà attenersi. Inoltre il responsabile del trattamento dovrà mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento, e dovrà tenere il registro dei trattamenti svolti (ex art. 30, paragrafo 2, GDPR).
Il responsabile ha, poi, l'obbligo di garantire la sicurezza dei dati adottando tutte le misure di sicurezza adeguate al rischio (art. 32 GDPR), tra le quali anche le misure di attuazione dei principi di privacy by design e by default, garantendo la riservatezza dei dati, vincolando i dipendenti, informando il titolare delle violazioni avvenute ed occupandosi della cancellazione dei dati alla fine del trattamento.

Nomina del Responsabile del trattamento dei dati personali

La nomina di ciascun Responsabile del trattamento dei dati personali deve essere effettuata dal Titolare del trattamento con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

7.3 Persona autorizzata al trattamento dei dati personali

Gli **Incaricati del trattamento** sono le persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali dal **Responsabile del trattamento**.

In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:
A tal fine, vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal titolare/responsabile;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
  - divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del titolare/responsabile;
  - l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
  - la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento degli interessati rilasciato in forma scritta;

- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

Nomina delle persone autorizzate al trattamento dei dati personali

La nomina di ciascuna **Persona autorizzata al trattamento dei dati personali** deve essere effettuata dal **Titolare** o dal **Responsabile del trattamento** con una **lettera di incarico** in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.

TABELLA DELLE PARTI COINVOLTE NELLA PROTEZIONE DEI DATI PERSONALI		
PARTE INTERESSATA	**COINVOLGIMENTO**	**ESIGENZE E ASPETTATIVE**
Titolare del trattamento	Assicura la conformità ai requisiti della normativa applicabile	Assicurare la conformità ai requisiti applicabili in materia di protezione dei dati personali. Valutare e trattare i rischi in materia di trattamento dei dati. Definire e attribuire ruoli e responsabilità in materia di trattamento dei dati personali internamente alla Società, Titolare del trattamento, e verso soggetti esterni che trattano dati per conto della stessa.
Responsabile esterno del trattamento	Soggetto esterno che tratta dati personali per conto del Titolare	Essere nominato Responsabile esterno del trattamento in conformità ai requisiti del GDPR. Ricevere dal Titolare istruzioni chiare e documentate in merito ai trattamenti da effettuare.
Referente interno del trattamento	Soggetto interno che tratta dati personali all'interno dell'Ordine	Essere strumento di accountability e controllo per conto del Titolare. Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Titolare e fornirle all'Autorizzato interno. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali.

		Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate (c.d. "controlli operativi") in materia di protezione dei dati personali.
Autorizzato (o Incaricato) interno al trattamento o	Tratta dati personali all'interno dell'Ordine (es. dipendente, collaboratore)	Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Titolare e/o dal Responsabile interno. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate ("controlli operativi") in materia di protezione dei dati personali.
Amministratore di sistema	Tratta dati personali all'interno dell'Ordine, essendo autorizzato dall'Ordine o dal Responsabile esterno	Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Titolare. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate ("controlli operativi") in materia di protezione dei dati personali.
Interessati al trattamento	Soggetto di cui sono trattati i dati personali	Ottenere dall'Ordine, Titolare del trattamento, che i trattamenti dei dati personali siano effettuati nel rispetto dei requisiti applicabili, con particolare rispetto ai principi. Essere informato sui trattamenti effettuati dall'Ordine. Poter esprimere il proprio consenso sui singoli trattamenti, ove necessario. Avere un punto di contatto facilmente utilizzabile per esercitare i propri diritti.
Autorità Garante Privacy	Vigilare sulla corretta applicazione dei requisiti normativi	Ricevere tempestive segnalazioni da parte dell'Ordine, Titolare del trattamento, in caso di incidenti o violazioni in

		materia di protezione delle informazioni. Ricevere collaborazione da parte dell'Ordine, nell'ambito delle richieste inerenti l'applicazione dei requisiti normativi.

8. VALUTAZIONE DEI RISCHI – METODOLOGIA UTILIZZATA

Per ogni attività di trattamento è stata eseguita la valutazione dei possibili scenari di rischio.
Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ **LR** ≤ 3)*
Medio - basso	*(4 ≤ **LR** ≤ 6)*
Rilevante	*(8 ≤ **LR** ≤ 12)*
Alto	*(15 ≤ **LR** ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

9. ISTRUZIONI OPERATIVE PREDISPOSTE DALL'ORDINE

9.1 ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

INDICE

9. Non osservanza della normativa aziendale.

PREMESSA

L'utilizzo delle risorse informatiche e telematiche dell'Ordine deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Ordine dei Periti Industriali delle Province di Ancona e Macerata ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

1. UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere all'Ordine, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dallo stesso Ordine, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Titolare*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare o dal *Responsabile dei sistemi informatici* della Ordine dei Periti Industriali delle Province di Ancona e Macerata. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ordine a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Titolare*.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Titolare.*

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Titolare* nel caso in cui vengano rilevati virus.

2. UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte

regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Titolare* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

3. GESTIONE DELLE PASSWORD
Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite da**l** *Titolare o dal Responsabile informatico.*
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Titolare.*
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al *Titolare*, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Titolare*.

4. UTILIZZO DEI SUPPORTI MAGNETICI
Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

5. UTILIZZO DI PC PORTATILI
L'utente è responsabile del PC portatile assegnatogli dal *Titolare* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, appuntamenti, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

6. USO DELLA POSTA ELETTRONICA
La casella di posta, assegnata dall'Ordine all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o

per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Ordine dei Periti Industriali delle Province di Ancona e Macerata deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'Ordine "know how" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Titolare*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

7. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI
Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Titolare*.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

8. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI
È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

9. NON OSSERVANZA DELLA NORMATIVA AZIENDALE
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

9.2 ISTRUZIONI OPERATIVE DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal

momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR e della normativa nazionale in vigore.

Per **"Violazione di dati**" si intende 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 (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

- violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.
-

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente**: la notifica al Garante non è obbligatoria.
- **Rischio presente**: è necessaria la notifica al Garante.
- **Rischio elevato**: In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà

un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un’elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

9.3 ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

INDICE

PREMESSA

Il presente capitolo contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali dell’Ordine dei Periti Industriali delle Province di Ancona e Macerata, conformemente al Regolamento (Ue) 2016/679 (GDPR) ed alla normativa nazionale in vigore. I dipendenti, i collaboratori, i consulenti,

i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso dell'Ordine diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Ordine.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e la normativa nazionale in vigore, si definisce:

- 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;
- 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 di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti

autorizzati;

- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

3. MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento sono:

- identificazione dell'interessato:
  al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;
- verifica del controllo dell'esattezza del dato e della corretta digitazione:
  al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;
- Norme logistiche per l'accesso fisico ai locali:
  I locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

4. ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).

Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

a. Gestione strumenti elettronici (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.

Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

• al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni

particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;

• Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;

• Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:

- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
- Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

• Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

• prima della riconsegna, rimuovere eventuali file ivi elaborati;

• non lasciarlo mai incustodito, soprattutto all'esterno dell'Ordine;

• per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. in mobile chiuso a chiave;

• in caso di furto di un portatile è necessario avvertire il Titolare o il consulente informatico, onde prevenire possibili intrusioni ai sistemi aziendali;

• in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;

• eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

b. Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

• tutela l'utilizzatore ed in generale l'Ordine da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;

• tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;

• è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun incaricato deve scegliere le password in base ai seguenti criteri:

• devono essere lunghe almeno otto caratteri;

• non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;

• devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;

• non devono essere uguali alle precedenti.

Per la corretta gestione della password è necessario:

• Almeno ogni 3/6 mesi è obbligatorio cambiare la password;

• Ogni password ricevuta va modificata al primo utilizzo;

• La password venga conservata in un luogo sicuro;

• Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;

• Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

c. Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dal Titolare o dal Responsabile Informatico. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

• Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;

• Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;

• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Titolare o dal Consulente informatico;

• Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

d. Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'Ordine e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza dell'Ordine e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

• Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;

• È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;

• La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:

• l'indirizzo del destinatario sia stato correttamente digitato,

• l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;

• nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

e. Gestione del salvataggio dei dati

- Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, devono essere eseguiti i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

- Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…). L'Incaricato deve verificare che i supporti informatici utilizzati

per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

f. Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati a cura del Titolare. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

g. Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Ordine è stato installato un software antivirus.

L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.

Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al titolare o al responsabile del Servizio Informatico.

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

5. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.

Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

a) distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

b) Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:

• la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
• la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti.

c) Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:
• in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
• la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
• l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
• i supporti devono essere archiviati in ambiente ad accesso controllato;
• i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
• il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
• cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
• l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
• la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
• ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
• quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
• l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

6. ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:
• Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
• gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione

dell'Amministratore di sistema;
• gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione del Titolare;
• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su indicazione del Titolare;
• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;
L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:
• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
• Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
• Per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
• Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
• E' necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
• Tutti i dati personali contenuti nei data base devono essere protetti da password;
• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:
o in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;
o in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.
• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi al Titolare o provvedere, in collaborazione con il Titolare stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
• l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
• E' assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;
• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

7. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

8. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.