DPA DATA PROTECTION AGREEMENT

ISTRUZIONI AL RESPONSABILE ESTERNO PER UN CORRETTO TRATTAMENTO DEI DATI PERSONALI.

1. SCOPO DEL DOCUMENTO

Lo scopo del presente documento è rappresentato dalla definizione e formalizzazione delle linee guida di recepimento delle disposizioni di legge in materia di trattamento di dati personali effettuato, con o senza l'utilizzo di strumenti elettronici, dalle strutture del Responsabile esterno del trattamento per conto di Mercurio Service S.p.A. (Titolare del trattamento).

In particolare, il documento definisce i criteri da adottare per l'individuazione delle figure coinvolte nel trattamento dei dati personali, così come definite dal Regolamento Europeo 2016/679/UE (nel seguito anche "GDPR") e dal Decreto Legislativo 196/2003 – Codice in materia di protezione dei dati personali (nel seguito anche "Codice Privacy"), per la definizione delle istruzioni, rivolte ai collaboratori del Responsabile, necessarie a garantire che il trattamento dei dati venga effettuato nell'osservanza dei limiti normativi e regolamentari vigenti, nonché per dare adempimento alle altre prescrizioni di legge.

Il documento costituisce il "Data Protection Agreement" con cui il Responsabile riceve le istruzioni per il trattamento dei dati, allegato alla clausola contrattuale di individuazione del rapporto, ai sensi dell'art. 28 del GDPR.

2. PRINCIPI DI RIFERIMENTO

La società Mercurio svolge il trattamento dei dati personali in ottemperanza a quanto previsto dal GDPR e dal Codice Privacy, nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità della persona, con particolare riferimento a riservatezza e identità personale.

Di conseguenza, i dati personali oggetto di trattamento da parte del Responsabile del trattamento, in conformità a quanto previsto dall'art. 5 del GDPR, dovranno essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti e registrati per scopi determinati, espliciti e legittimi e utilizzati in altre operazioni di trattamento in termini compatibili con tali scopi,
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

3. RIFERIMENTI

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 – Regolamento generale sulla protezione dei dati (GDPR)
- Decreto Legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali
- Provvedimenti, linee guida e autorizzazioni dell'Autorità Garante per la protezione dei dati personali (nel seguito "Garante"), disponibili sul sito dell'Autorità (http://www.garanteprivacy.it)

4. DEFINIZIONI

Trattamento

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco comunicazione, diffusione, cancellazione e distribuzione dati.

Dati personali

Qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati identificativi

I dati personali che permettono l'identificazione diretta dell'interessato.

Dati sensibili (art. 9 GDPR)

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

Dati giudiziari (art. 10 GDPR)

I dati personali idonei a rivelare provvedimenti giudiziari.

Dati comuni

I dati personali diversi da quelli sensibili e giudiziari.

Titolare

Persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, cui competono le decisioni in ordine alle finalità, modalità del trattamento dei dati personali ed agli strumenti utilizzati ivi compreso il profilo della sicurezza.

Responsabile esterno

Persona fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione o organismo preposti dal titolare del trattamento di dati personali.

Incaricati

Persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato

Persona fisica cui si riferiscono i dati personali.

5. DESCRIZIONE DEL PROCESSO

5.1. PROTOCOLLI

Nell'esecuzione delle proprie mansioni, dovranno essere rispettati i seguenti protocolli operativi.

5.2. PROTOCOLLO ESIBIZIONE INFORMATIVE E ACQUISIZIONE CONSENSI

Il Titolare del trattamento ha l'obbligo di fornire agli interessati adeguate informazioni circa i trattamenti effettuati. A tal fine, il Responsabile del trattamento, se è necessario fornire la cd "informativa privacy" di Alfa spa, per esempio a richiesta degli interessati, dovrà avere cura di fornire tali informazioni, prima di iniziare il relativo trattamento:

- mediante spedizione di copia della pertinente informativa via e-mail, fax o posta direttamente all'interessato, in base alle sue richieste;
- mediante esibizione e/o lettura dell'informativa generale all'interessato che richieda di ricevere le informazioni solo oralmente;
- mediante acclusione della stessa ai documenti utilizzati e in occasione di eventi pubblici promozionali, organizzati da o a favore di Alfa.

Dovrà essere garantita l'archiviazione delle varie versioni succedutesi nel tempo, da mettere eventualmente a disposizione dell'interessato.
Sarà cura di ciascun Responsabile del trattamento consegnare le informative aggiornate, non appena ricevuta notizia della loro modifica.
Dovrà essere cura del Responsabile del trattamento di acquisire il consenso degli interessati, ove necessario, annotando l'eventuale revoca del consenso.

6. GLI AUTORIZZATi AL TRATTAMENTO DEI DATI

Il trattamento dei dati personali deve essere effettuato solo da soggetti che hanno una relazione qualificata con il Responsabile del trattamento, sulla base di idonee istruzioni.
Oltre alle istruzioni generali su come devono essere trattati i dati, agli Incaricati vengono assegnati specifiche funzioni in merito ai seguenti punti, ai fini della sicurezza:
A - Procedure da seguire per la classificazione dei dati personali, con specifiche indicazioni per i dati sensibili e giudiziari, garantendo per tutti questi gli standard di sicurezza opportuni ed idonei;
B - Modalità di reperimento dei documenti contenenti i dati personali e modalità da osservare per la custodia degli stessi e la loro archiviazione al termine dei lavori;
C - Modalità per elaborare e custodire le password necessarie per accedere ai personal computer e ai dati in essi contenuti, nonché per fornire una copia della parola chiave al preposto alla custodia solo nei casi di assenza conformemente al Disciplinare sull'uso degli strumenti digitali, allegato al presente documento.
D - Prescrizioni per non lasciare incustoditi o accessibili i personal computer mediante:
1. Disconnessione utente;
2. Procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informatici;
3. Modalità di custodia e utilizzo dei supporti rimuovibili contenenti dati personali;
4. Dovere di aggiornarsi utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Al fine della corretta gestione dei dati in trattamento, il Responsabile esterno del trattamento deve prescrivere all'incaricato di attenersi alle seguenti istruzioni:

- trattare i dati in modo lecito e secondo correttezza e secondo le prescrizioni del Reg. 2016/679/UE (c.d. GDPR);
- raccogliere e registrare i dati per gli scopi inerenti all'attività svolta;
- verificare, ove possibile, che siano esatti e, se necessario, aggiornarli;
- verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, trattando solo i dati necessari per l'espletamento delle mansioni di propria competenza;
- custodire e non divulgare il codice di identificazione personale (username) e la password di accesso agli strumenti elettronici;
- non lasciare incustodito il proprio posto lavoro prima di aver provveduto alla messa in sicurezza dei dati;
- non lasciare incustoditi e accessibili a terzi gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza esplicita autorizzazione del Responsabile;
- mantenere la massima riservatezza sui dati predetti se non previamente autorizzato dal Responsabile del trattamento;
- osservare tutte le misure di protezione e sicurezza, già in atto o successivamente disposte, atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, o trattamento non consentito dei dati personali;
- non tentare di acquisire i Privilegi di Amministratore di sistema, non accedere a servizi non consentiti, non eseguire software non autorizzati, non usare supporti infetti da virus;
- consegnare al Responsabile o all'Amministratore di Sistema i supporti informatici o ottici contenenti dati personali non più utilizzabili o la cui memoria sia esaurita, evitando di smaltirli in autonomia o perderli;
- informare il Responsabile e, eventualmente, l'Amministratore di Sistema in caso di incidenti relativi alla sicurezza dei dati;
- comunicare i dati a soggetti terzi, solo ove ciò sia funzionale allo svolgimento dei compiti affidati e, comunque, tramite strumenti digitali di diretto controllo (mail, telefoni e fax aziendali) e mai tramite strumenti di terzi (es. social network, mail private, chat private, messaggistica istantanea, etc.);
- trasmettere la documentazione cartacea tra uffici, contenente dati personali, in buste chiuse o modalità simili per evitarne la rivelazione;
- riporre la documentazione cartacea negli appositi archivi ad accesso controllato e, se necessario distruggerla, farlo in modo che sia adeguatamente sminuzzata di talché sia resa inintelligibile;
- accertarsi dell'identità del diretto interessato richiedente, prima di fornire informazioni circa i dati personali o il trattamento effettuato;
- conservare i dati trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono raccolti e successivamente trattati.

Nel caso di presenza di ospiti o personale di servizio sarà necessario:
- fare attendere in luoghi in cui non sono presenti informazioni riservate o dati personali;
- evitare di allontanarsi dalla scrivania in presenza di ospiti o riporre i documenti e attivare il salvaschermo del PC, previo blocco dello stesso con password;
- non rivelare o far digitare la password al personale di assistenza tecnica;
- non rivelare le password al telefono, né inviarle via fax, mail, chat, social network o altri sistemi;

- segnalare qualsiasi anomalia e stranezza al Responsabile.

Misure specifiche per quanto riguarda i dati sensibili e giudiziari:
- non fornire dati o informazioni di carattere sensibile per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
- evitare di inviare, per fax e-mail, documenti in chiaro contenenti dati sensibili: in tal caso, la documentazione dovrà essere inviata, se necessario, senza alcun esplicito riferimento all'interessato (ad esempio, contrassegnando i documenti semplicemente con un codice);
- i documenti, ancorché non definitivi, ed i supporti recanti dati sensibili o giudiziari, devono essere conservati, anche in corso di trattamento, in elementi di arredo muniti di serratura e non devono essere lasciati incustoditi in assenza dell'incaricato.

6.1. DOVERI DELL'AUTORIZZATO

L'Autorizzato dovrà rispettare le istruzioni impartite dal Responsabile del trattamento.
In particolare, dovrà:

- procedere alla raccolta di dati personali, anche mediante l'approvazione di appositi moduli di raccolta digitalizzati;
- consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa, salvo che l'informativa medesima sia stata fornita direttamente dal titolare o dal responsabile ovvero non sia necessario consegnarla;
- raccogliere, sempre al momento della raccolta dei dati, il consenso espresso, documentato per iscritto, degli interessati ai trattamenti previsti, salvo che a ciò abbiano provveduto direttamente il titolare o il responsabile, e salvo i casi di esonero dal consenso previsti dalla stessa legge;
- trattare i dati personali in modo lecito e secondo correttezza, nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti;
- verificare, ove possibile, che siano esatti e provvedere, se necessario, al loro aggiornamento;
- verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare o dal Responsabile del Trattamento;
- adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal Titolare o dal Responsabile del trattamento, in particolare dovrà eseguire quanto di seguito precisato:

a. per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
b. trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
c. conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
d. con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
e. copie di dati personali su supporti amovibili sono permesse solo se parte del trattamento, copie di dati sensibili devono essere espressamente autorizzate. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;

f. in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Responsabile del trattamento e all'Amministratore di sistema;

- segnalare al Titolare o al Responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle già menzionate misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- effettuare la comunicazione e la diffusione dei dati esclusivamente ai soggetti indicati dal Titolare o dal Responsabile e secondo le modalità stabilite dai medesimi;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
- svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dal Titolare e dal Responsabile e, comunque, in modo lecito e secondo correttezza;
- fornire al Titolare o al Responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al Titolare ed al Responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- rispettare, nella conservazione, le misure di sicurezza predisposte. In ogni operazione di trattamento dovrà essere garantita la massima riservatezza;
- verificare, in caso di allontanamento anche temporaneo dal posto di lavoro, che terzi, anche se dipendenti, non possano accedere a dati non di loro pertinenza chiudendo classificatori, cassetti e porta dell'ufficio dove i dati vengono mantenuti ed inserendo password su salvaschermo del PC;
- consegnare i documenti direttamente all'interessato utilizzando cartelline o buste non trasparenti.

6.2. LINEE GUIDA PER LA SICUREZZA GENERALE

Il Responsabile del trattamento dovrà assicurarsi che i propri collaboratori adottino le seguenti misure di sicurezza comportamentali o istruzioni similari (qualora già elaborate all'interno del proprio "protocollo privacy").

1. Utilizzare le chiavi

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo.

2. Attenzione ai documenti importanti

I documenti importanti dal punto di vista della privacy, sia informatici che cartacei, è opportuno che vengano archiviati negli appositi luoghi dotati di sistema di sicurezza al termine della giornata lavorativa, mentre durante l'attività devono essere custoditi con attenzione per evitare che possano essere letti da estranei anche in vostra presenza.

3. Uso di carta riciclata

L'uso di carta riciclata è sicuramente una buona prassi, alla quale però è necessario prestare molta attenzione in caso di presenza di dati personali.

4. Distruzione dei documenti

Quando ci si deve disfare di documenti contenenti dati personali, farlo in modo che i dati ivi contenuti risultino totalmente illeggibili, ad esempio mediante sminuzzatori e trita-documenti.

5. Conservazione dei documenti

I documenti contenenti dati personali devono essere conservati in modo tale da evitarne l'accesso a chi non è autorizzato. Devono altresì essere resi disponibili in caso di richiesta da parte dell'interessato, ma solo dietro specifica autorizzazione del Responsabile del Trattamento ed entro i limiti stabiliti dalla Legge. La conservazione sostitutiva dei documenti digitali deve garantire la protezione dei dati e delle procedure informatiche, ovvero garantire tutte le misure necessarie per la sicurezza fisica, logica e ambientale dei dati e del sistema preposto alla loro conservazione (comprensivo delle copie di sicurezza dei supporti di memorizzazione), garantire la tutela della privacy attraverso un trattamento a norma di dati e informazioni personali, etc.

6. Certificati e documenti vari

Limitare la produzione di modulistica troppo vasta contenete campi quali "altro" che richiedono dati eccedenti, che esulano dalla finalità della richiesta stessa.

7. Certificati medici vari

Certificati di malattia, certificati di pronto soccorso e tutta la documentazione inerente allo stato di salute di un interessato contengono "dati sensibili" devono essere trattati con una disciplina ancora più stringente rispetto al "dato personale". Se un dipendente/utente consegna un certificato medico, non va lasciato sulla scrivania e va portato al più presto all'Ufficio competente.

La sicurezza informatica

1. Conservare i supporti di memorizzazione in un luogo sicuro

Per i supporti di memorizzazione eventualmente utilizzati si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sottochiave non appena avete finito di usarli.

2. Utilizzare le password

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

- La password di accesso al computer impedisce l'utilizzo improprio della propria postazione, quando per un motivo o per l'altro non ci si trova in ufficio.
- La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
- La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
- La password del salvaschermo, infine, impedisce che un'assenza momentanea permetta a una persona non autorizzata di visualizzare il lavoro. Scegliere le password secondo le indicazioni fornite dall'Amministratore del Sistema.

3. Attenzione alle stampe di documenti riservati

Non lasciare accedere persone non autorizzate ai documenti informatici presenti nei PC, né ad eventuali stampe cartacee di documenti; se la stampante non si trova sulla scrivania recarsi quanto prima a ritirare le stampe. Distruggere personalmente le stampe quando non servono più con il distruggi documenti.

4. Non lasciare traccia dei dati riservati

5. Prestare attenzione all'utilizzo dei PC portatili

I PC portatili sono un facile bersaglio per i ladri. Se c'è necessità di gestire dati riservati su un portatile, è possibile installare un buon programma di cifratura del disco rigido e utilizzare una procedura di backup periodico.

6. Custodire le password in un luogo sicuro

Il post-it sullo schermo non è un luogo sicuro, né altri fogli volanti: le password devono essere custodite separatamente dal dispositivo cui accedono.

7. Non fare usare il computer a personale esterno a meno di non essere sicuri della loro identità e autorizzazione ad accedervi

Ad esempio, verificare che si tratti del personale chiamato a eseguire la manutenzione dietro specifica autorizzazione del titolare o del responsabile del trattamento.

8. Non utilizzare apparecchi non autorizzati

L'utilizzo di modem senza una specifica autorizzazione su postazioni di lavoro collegati alla rete offre una porta d'accesso dall'esterno non solo al computer, ma a tutta la Rete, ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultarsi con il responsabile IT.

9. Non installare programmi non autorizzati

Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il lavoro richiede l'utilizzo di programmi specifici, consultarsi con il responsabile IT.

10. Applicare con cura le linee guida per la prevenzione da infezioni di virus

La prevenzione da virus sul computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, si potrebbe incorrere in una perdita irreparabile di dati.

11. Controllare la politica locale relativa ai backup

Evitare di registrare nel disco locale informazioni sensibili e non in quanto esse non vengono salvate e, a fronte di un guasto tecnico, irrimediabilmente perse. La registrazione sulle unità di rete invece avviene in sicurezza in quanto i dati vengono salvati regolarmente.

Linee guida per la prevenzione dei virus

1. Usare soltanto programmi provenienti da fonti fidate

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. Proteggere i dispositivi da scrittura quando possibile

In questo modo si evitano le sovrascritture accidentali, magari tentate da un virus che tenta di propagarsi. virus non possono in ogni caso aggirare la protezione meccanica.

3. Assicurarsi che il software antivirus sia aggiornato

4. Non diffondere messaggi di provenienza dubbia

5. Non partecipare a "catene di S. Antonio" e simili

6. Mail truffa e phishing

È ormai molto diffusa la pratica del "phishing", ossia la ricezione di e-mail che risultano molto simili a comunicazioni istituzionali di Enti Pubblici (es. Agenzia delle Entrate) oppure da privati incaricati di pubblici servizi (es. gestore telefonia): tali e-mail sono, in realtà, tentativi di truffa o di accesso illegale alla casella e-mail. Di solito, tali comunicazioni avvertono di un mancato pagamento oppure di una vincita in denaro o comunque contengono inviti a fornire le credenziali di accesso proprie o dell'azienda oppure le credenziali delle carte di credito o di conti in banca. Evitare assolutamente di rispondere a tali comunicazioni e, nei casi dubbi, consultarsi con l'Amministratore di sistema e con il Responsabile del trattamento.

7. MODULISTICA

DPS_PRIVACY_POLICY_REV.1_20220420