LPD
Legge Federale sulla protezione dei dati

Matteo Colombo

Roberta De Giusti

INDICE

LA LPD | LEGGE FEDERALE SULLA PROTEZIONE DEI DATI

1

A

INTRODUZIONE NORMATIVA

INTRODUZIONE NORMATIVA E LEGGE SULLA PROTEZIONE DEI DATI (LPD)

19 giugno 1992

Legge federale sulla protezione dei dati (LPD)

01 aprile 2015

revisione (totale) della Legge sulla protezione dei dati personali

LPD adottata 25 settembre 2020

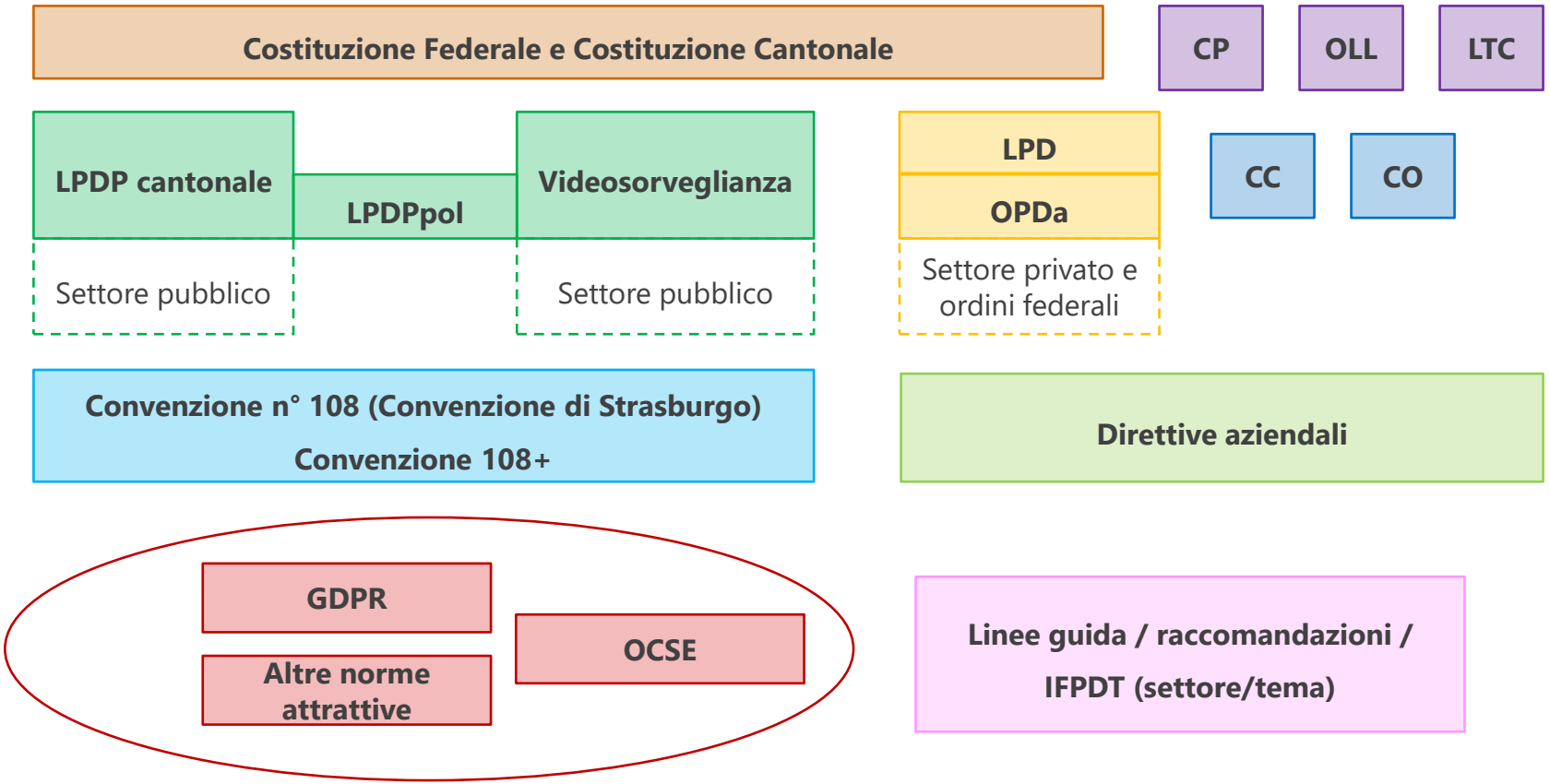
Entrata in vigore il 1 settembre 2023

INTRODUZIONE NORMATIVA E LEGGE SULLA PROTEZIONE DEI DATI (LPD)

L'obiettivo generale è di modernizzare la LPD e di adeguarla al diritto europeo affinché l'UE continui a riconoscere la Svizzera come uno Stato terzo con una protezione dei dati adeguata, in modo da consentire anche in futuro la comunicazione transfrontaliera di dati.

Scopo della LPD è ***proteggere la personalità e i diritti fondamentali delle persone i cui dati personali sono oggetto di trattamento.***

FONTI DEL DIRITTO SULLA PROTEZIONE DEI DATI UE



AMBITO DI APPLICAZIONE | ART. 2 LPD

Campo d'applicazione personale e materiale

Si

Al trattamento di dati personali **concernenti persone fisiche da parte di**:

a. **Privati**;

b. **Organi federali**.

No

Al trattamento di dati personali da parte:

a. Di **persone fisiche per uso esclusivamente personale**;

b. Delle **camere federali** e delle **commissioni parlamentari** nell'ambito delle loro **deliberazioni**

c. Dei **beneficiari istituzionali** [...] che godono dell'immunità di giurisdizione in svizzera.

AMBITO DI APPLICAZIONE | ART. 3 LPD

Campo d’applicazione territoriale

Si applica alle **fattispecie che generano effetti in svizzera**, **anche se si verificano all’estero**.

B

DEFINIZIONI

DEFINIZIONI

Protezione dei dati personali?

Dato personale?

Comunicazione?

Diffusione?

Interessato?

Trattamento?

DEFINIZIONI

«Dati personali degni di particolare protezione» - «dati sensibili»

Razza o origine etnica

Opinioni politiche

Credo religioso | filosofico

Iscrizione a sindacati

Salute | Misure assistenza sociale

Orientamento sessuale Sfera intima

Dati genetici

Dati biometrici

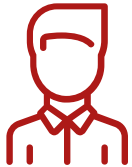
Misure di assistenza sociale

Perseguimenti e sanzioni amministrativi e penali

C

I SOGGETTI

TITOLARE E RESPONSABILE DEL TRATTAMENTO



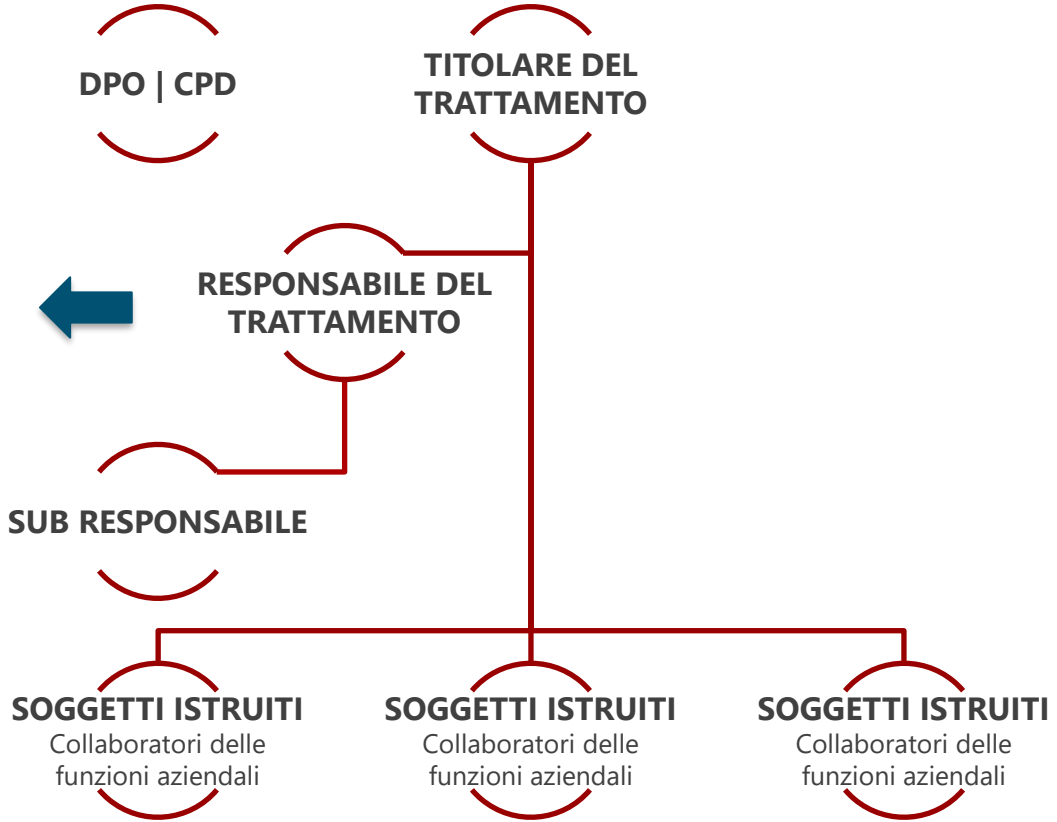
Titolare del trattamento (Art. 5 LPD) è:

il privato o l'organo federale che, singolarmente o insieme ad altri, determina lo ***scopo*** e i ***mezzi*** del trattamento.

Responsabile del trattamento (Art. 5 LPD) è:

il privato o l'organo federale che ***tratta dati personali per conto del titolare del trattamento***.

ORGANIGRAMMA PRIVACY | LPD

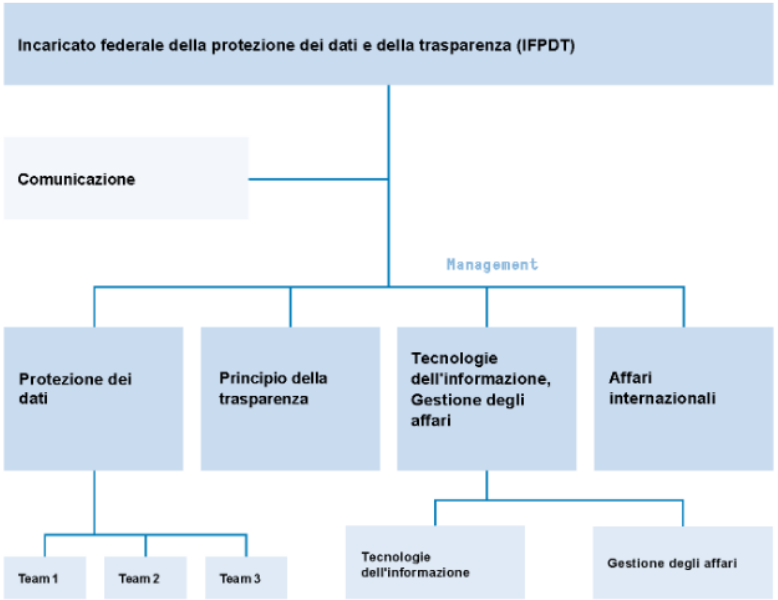


Esempi: il fornitore che elabora i salari, il fornitore che si occupa dell'assistenza informativa

I dipendenti del titolare del trattamento che trattano dati di clienti, dipendenti, fornitori

INCARICATO FEDERALE | IFPDT

Organigramma



(Stato 31 marzo 2023)

INCARICATO FEDERALE | IFPDT

I principali compiti

Informare, formare e consigliare gli organi federali e i privati in questioni concernenti la protezione dei dati

Assistere gli organi cantonali e collaborare con le autorità svizzere ed estere competenti in materia di protezione dei dati

Sensibilizzare il pubblico, soprattutto le persone vulnerabili, alla protezione dei dati

Informare, su richiesta, le persone interessate in merito all'esercizio dei loro diritti

Elaborare strumenti di lavoro sotto forma di **raccomandazioni di buona prassi** per i titolari del trattamento, i responsabili del trattamento e le persone interessate

IL RUOLO DEL CPD/DPO NELLA LPD

I titolari privati del trattamento possono nominare un consulente per la protezione dei dati. (art. 10, cpv 1, LPD). Compiti del consulente:

Funge da **interlocutore** per le **persone interessate**

Funge da **interlocutore per le autorità** competenti in svizzera per la protezione dei dati (IFPDT)

Partecipa all'applicazione delle disposizioni sulla protezione dei dati

Fornisce **formazione e consulenza** al titolare privato del trattamento in questioni concernenti la protezione dei dati

Se richiesto, **fornisce il suo parere sulla** valutazione d'impatto sulla protezione dei dati (**DPIA**).

IL RUOLO DEL CPD/DPO NELLA LPD

Il titolare può rinunciare a consultare l'IFPDT in sede di **valutazione d'impatto sul trattamento dei dati | DPIA** (art. 10, cpv 3, LPD) se:

- Il consulente (CPD | DPO) esercita la sua funzione in modo indipendente dal titolare del trattamento e senza ricevere da questi istruzioni;
- Il consulente non esercita attività inconciliabili con i suoi compiti di consulente;
- Il consulente dispone delle conoscenze tecniche necessarie;
- Il titolare del trattamento pubblica i dati di contatto del consulente e li comunica all'IFPDT.

GLI ISTITUTI E I DOCUMENTI NECESSARI

2

ELENCO DELLE ATTIVITA' DA SVOLGERE

COMPLIANCE	Analisi delle misure di sicurezza tecniche / fisiche / organizzative
	Registri dei trattamenti (titolare e/o responsabile) ed analisi dei rischi
	Mappatura dei fornitori (responsabili) e redazione delle clausole privacy da inserire nei contratti con i fornitori
	Predisposizione/aggiornamento delle principali informative (dipendenti/candidati/clienti/fornitori)
	Redazione della procedura per la gestione delle violazioni di dati personali

ELENCO DELLE ATTIVITA' DA SVOLGERE

COMPLIANCE	Formazione e sensibilizzazione del personale
	Compliance della vetrina della Società - IL SITO INTERNET - (Privacy policy e cookie policy)
	Verifica dei sistemi di potenziale controllo lavoratori (es. videosorveglianza – GPS – Posta elettronica – Telefoni aziendali) e Regolamento sul corretto utilizzo degli strumenti aziendali
	DPIA – Valutazione d'impatto sulla protezione dei dati (da valutare, se necessaria, in base ai trattamenti)

A

REGISTRO DEI TRATTAMENTI

REGISTRO DEI TRATTAMENTI

Art. 12 LPD

Il **registro del responsabile** del trattamento contiene indicazioni in merito alla sua identità e a quella del titolare del trattamento, alle categorie dei trattamenti eseguiti su incarico del titolare del trattamento, come pure le indicazioni di cui al capoverso 2 lettere f e g.

Il Consiglio federale prevede eccezioni per le **imprese con meno di 250 collaboratori** i cui trattamenti di dati personali comportano soltanto un rischio esiguo di violazione della personalità delle persone interessate.

REGISTRO DEI TRATTAMENTI

Scopo del trattamento	**Gestione del rapporto con i clienti| adempimento degli obblighi precontrattuali e contrattuali**
Contitolare del trattamento	//
Categorie dei soggetti interessati	Clienti
Categorie dei destinatari	Fornitore software gestionale Fiduciaria Revisori contabili
Dati personali trattati	Dati personali, Dati anagrafici, Dati bancari, Dati identificativi, Dati di contatto
Dati degni di particolare protezione trattati	//
Paesi extra Confederazione Svizzera in caso di comunicazioni all'estero	Germania
Garanzie adeguate	Paese considerato adeguato dal Consiglio Federale
Tempo di conservazione	Successivamente alla conclusione del rapporto contrattuale, i dati saranno conservati per 10 anni
Misure volte alla sicurezza dei dati	Password cambiata al primo accesso, Password composta da almeno 8 caratteri, Password di complessità alfanumerica con caratteri speciali, Antivirus, Backup, Protezione da malicious software
Informazioni ulteriori	
Motivi giustificativi	Contratto

COME FARLO?

Interviste con ai referenti di funzione (ad esempio, ufficio del personale, segreteria, IT) per:

- acquisire informazioni sui dati personali trattati, lo scopo del trattamento, gli strumenti utilizzati, i fornitori…
- Acquisire documenti privacy

Creazione del flusso:

- Organigramma privacy
- asset/strumenti/applicativi
- ubicazione dei dati
- mappatura dei fornitori

Identificazione delle finalità di trattamento: es. Selezione del personale

- Dati personali raccolti, anche degni di particolare protezione.
- Interessati (dipendenti etc.).
- Comunicazione dei dati e trasferimento dati.
- Principali misure di sicurezza adottate
- Tempistiche di conservazione

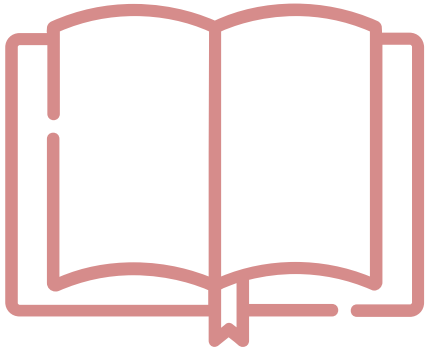
B

INFORMATIVE PRIVACY

INFORMATIVE PRIVACY

Il titolare del trattamento comunica alla persona interessata le informazioni sull'ottenimento di dati personali in forma precisa, trasparente, comprensibile e facilmente accessibile.

Non sono fornite ulteriori indicazioni sull'informativa privacy il cui contenuto è già previsto all'art. 19 nLPD.

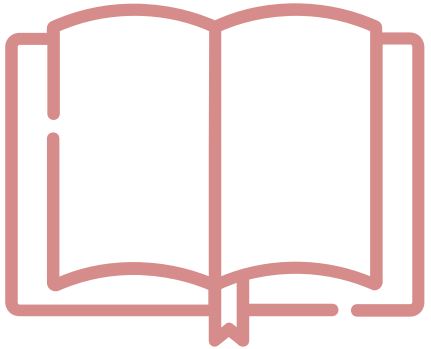


Art. 13 OPDa

INFORMATIVE PRIVACY

Se i dati personali non sono raccolti presso la persona interessata, il titolare del trattamento la informa inoltre sulle categorie di dati personali trattati.

- l'identità e i dati di contatto del titolare del trattamento
- lo scopo del trattamento
- i destinatari o le categorie di destinatari cui sono comunicati dati personali
- comunicazione di dati personali all'estero



Art. 13 OPDa

INFORMATIVE PRIVACY

2. IDENTITÀ E CONTATTI DEL TITOLARE DEL TRATTAMENTO

Il soggetto che determina le finalità e i mezzi del presente trattamento di dati personali è _____ *[inserire ragione sociale del titolare del trattamento]* (nel seguito definita anche "Titolare" o "Società").

Il Titolare del trattamento può essere contattato al seguente indirizzo: _____ *[inserire dato di contatto del titolare, casella e-mail @privacy, se presente]*

3. FINALITÀ DEL TRATTAMENTO | PERIODO DI CONSERVAZIONE DEI DATI

FINALITÀ DEL TRATTAMENTO	PERIODO DI CONSERVAZIONE DEI DATI
a) gestione del rapporto con i clienti| adempimento degli obblighi precontrattuali e contrattuali: i dati personali saranno usati per instaurare e/o dare esecuzione al rapporto contrattuale con il cliente	Successivamente alla conclusione del rapporto contrattuale, i dati saranno conservati per 10 anni
b) recupero crediti giudiziale e stragiudiziale | gestione eventuale contenzioso	Successivamente alla conclusione del rapporto di contrattuale, i dati saranno conservati per 10 anni. In Caso di contenzioso, i dati saranno conservati sino alla conclusione dello stesso.
b) newsletter, invio di e-mail promozionali/pubblicitarie con contenuto analogo ai prodotti e servizi già forniti da _____ *[inserire ragione sociale del titolare del trattamento]* al cliente (soft spam)	Fino ad opposizione del cliente

C

NOMINA DEI RESPONSABILI DEL TRATTAMENTO

RESPONSABILE DEL TRATTAMENTO

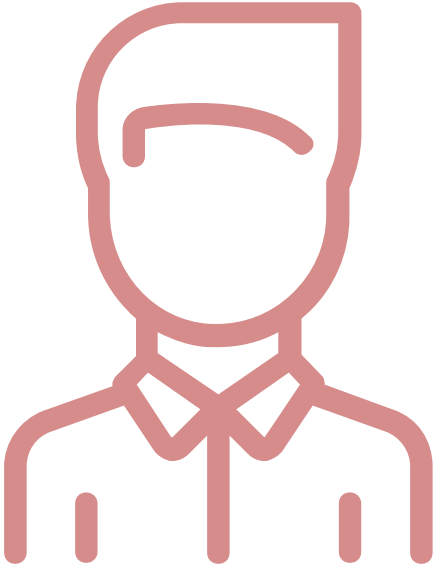
Art. 9 LPD

Trattamento di dati personali da parte di un responsabile

1. Il trattamento di dati personali può essere affidato a un responsabile del trattamento per contratto o per legge se:
   a. questi effettua soltanto i trattamenti che il titolare del trattamento avrebbe il diritto di effettuare; e
   b. nessun obbligo legale o contrattuale di serbare il segreto lo vieta.

RESPONSABILE DEL TRATTAMENTO

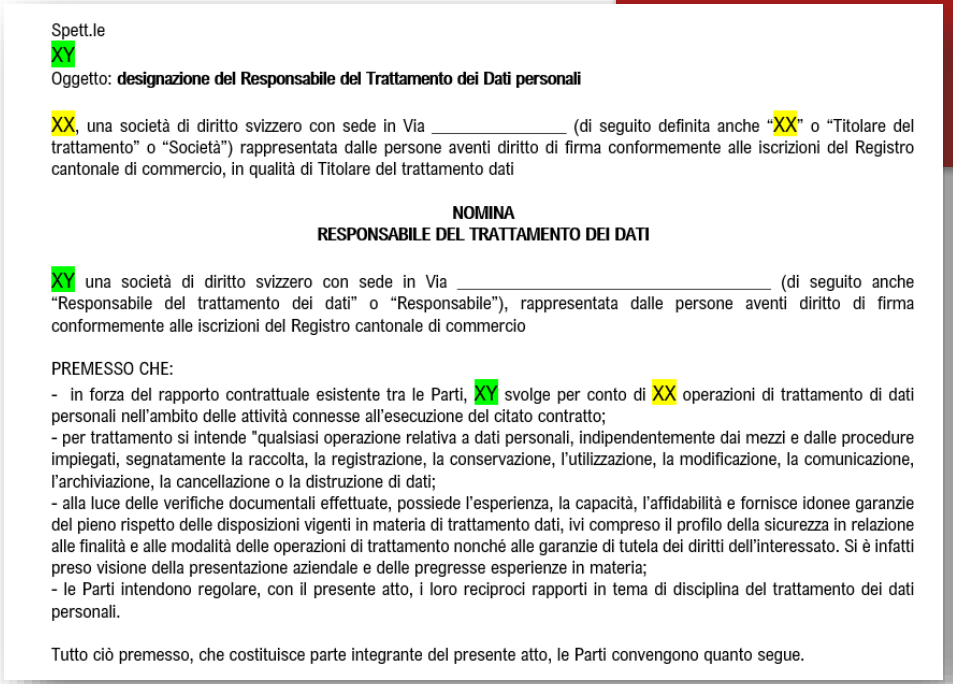
2. Il titolare del trattamento deve in particolare assicurare che il responsabile del trattamento sia in grado di garantire la sicurezza dei dati.
3. Il **responsabile del trattamento può affidare il trattamento a un terzo soltanto previa autorizzazione del titolare del trattamento.**
4. Il responsabile del trattamento può far valere gli stessi motivi giustificativi del titolare del trattamento



RESPONSABILE DEL TRATTAMENTO

I PRINCIPALI FORNITORI CHE TRATTANO DATI SU ISTRUZIONE DEL TITOLARE:

- Fiduciaria che elabora i salari;
- Fornitori che si occupano dell'assistenza / manutenzione di software / gestionali / applicativi;
- Fornitori di servizi di hosting e data center;
- Fornitori che presidiano l'impianto di videosorveglianza.



Spett.le
XY
Oggetto: **designazione del Responsabile del Trattamento dei Dati personali**

XX, una società di diritto svizzero con sede in Via _____ (di seguito definita anche "XX" o "Titolare del trattamento" o "Società") rappresentata dalle persone aventi diritto di firma conformemente alle iscrizioni del Registro cantonale di commercio, in qualità di Titolare del trattamento dati

NOMINA
RESPONSABILE DEL TRATTAMENTO DEI DATI

XY una società di diritto svizzero con sede in Via _____ (di seguito anche "Responsabile del trattamento dei dati" o "Responsabile"), rappresentata dalle persone aventi diritto di firma conformemente alle iscrizioni del Registro cantonale di commercio

PREMESSO CHE:
- in forza del rapporto contrattuale esistente tra le Parti, XY svolge per conto di XX operazioni di trattamento di dati personali nell'ambito delle attività connesse all'esecuzione del citato contratto;
- per trattamento si intende "qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la registrazione, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione, la cancellazione o la distruzione di dati;
- alla luce delle verifiche documentali effettuate, possiede l'esperienza, la capacità, l'affidabilità e fornisce idonee garanzie del pieno rispetto delle disposizioni vigenti in materia di trattamento dati, ivi compreso il profilo della sicurezza in relazione alle finalità e alle modalità delle operazioni di trattamento nonché alle garanzie di tutela dei diritti dell'interessato. Si è infatti preso visione della presentazione aziendale e delle pregresse esperienze in materia;
- le Parti intendono regolare, con il presente atto, i loro reciproci rapporti in tema di disciplina del trattamento dei dati personali.

Tutto ciò premesso, che costituisce parte integrante del presente atto, le Parti convengono quanto segue.

RESPONSABILE DEL TRATTAMENTO

Perché è importante il presidio e la contrattualizzazione del fornitore che tratta dati?

- Marzo 2021. I datacenter di OVH (azienda di web hosting leader nel settore con 1,5 milioni di clienti nel mondo) vanno in fiamme. Verificatosi a Strasburgo, l'incendio ha distrutto uno dei datacenter più grandi d'Europa.

- L'incidente ha avuto origine dal datacenter SBG2 e si è diffuso su tutte le altre unità SBG1, SBG3 e SGB4. Nonostante l'arrivo tempestivo dei vigili del fuoco, non è stato possibile domare le fiamme all'interno delle unità del datacenter.

- L'incendio a Strasburgo ha portato offline siti e servizi in diverse città ad esempio italiane.

RESPONSABILE DEL TRATTAMENTO

- OVH non aveva previsto un piano generale di Data Recovery

Conseguenza → in mancanza di un back up dei dati o di un recovery plan gestito direttamente dal titolare, i dati contenuti nei server distrutti sono andati persi, forse per sempre.

- il servizio di Recovery Plan di OVH era previsto come servizio a parte per i clienti (anche il backup), da acquistare in aggiunta ai servizi di base

RESPONSABILE DEL TRATTAMENTO

Sarebbe bastato acquistare il servizio aggiuntivo?

NON è detto

OVH, nelle proprie condizioni generali di contratto, declina ogni responsabilità circa la buona esecuzione del backup, lasciando al cliente il compito di verificare il backup realizzato e quali siano le cause di un eventuale fallimento della procedura.

D

MISURE DI SICUREZZA

SICUREZZA DEI DATI | ART. 8 LPD

Il titolare e il responsabile del trattamento garantiscono, mediante appropriati **provvedimenti** tecnici e organizzativi, che la sicurezza dei dati personali **sia adeguata al rischio**. I provvedimenti devono permettere di evitare violazioni della sicurezza dei dati. Il Consiglio federale emana disposizioni ***sui requisiti minimi in materia di sicurezza dei dati***.

MISURE DI SICUREZZA | ESEMPI

- **Formazione** e sensibilizzazione del personale
- La **pseudonimizzazione**
- **Crittografia**
- **Firewall, antivirus**
- **Back up**, **disaster recovery plan, business continuity plan**
- Strumenti quali **MDM** per la gestione di dispositivi mobili
- Implementazione di **password** e cambio password (in alcuni casi **autenticazione a piu' fattori**)
- **Limitazione degli accessi ai sistemi** (profondità e profilazione delle utenze che possono accedere a determinate cartelle di rete o applicativi), **ai locali** (es. chiusura archivi, sale server etc.)
- **Vulnerability assessment**
- **Redazione e pubblicizzazione di procedure interne** (es. data breach policy, regolamento uso strumenti aziendali)

ART. 1 OPDa | PRINCIPI

Criteri per la valutazione del RISCHIO

a. Cause del rischio

b. Pericolo sostanziale

c. Provvedimenti adottati o previsti per minimizzare il rischio

d. Probabilità e gravità di una violazione della sicurezza dei dati nonostante i provvedimenti adottati o previsti

ART. 1 OPDa | PRINCIPI

Il titolare e il responsabile del trattamento devono definire la ***necessità di protezione dei dati personali*** e stabilire i ***provvedimenti tecnici e organizzativi adeguati in considerazione del rischio*.**

Criteri per la valutazione della NECESSITA' DI PROTEZIONE

a. Tipo di dati trattati

b. Scopo, tipo, portata e circostanze del trattamento

c. Lo stato della tecnica

d. Le spese di implementazione

LE MISURE DI SICUREZZA

La formazione / sensibilizzazione ed ISTRUZIONE del personale

Ordinanza sulla protezione dei dati (OPDa) - rapporto esplicativo

Art. 1 principi

Per garantire la sicurezza dei dati vi sono diversi provvedimenti. Eccone tre a titolo esemplificativo:

[…]

La **formazione** e la **consulenza delle persone incaricate di attuare i provvedimenti**: il consiglio federale ritiene importante la presente misura, perché **l'attuazione** e ***l'efficacia della sicurezza dei dati dipende in particolare anche dalle persone che applicano i provvedimenti stabiliti***. Infatti una formazione e una consulenza lacunose possono causare una violazione della sicurezza dei dati. I collaboratori vanno ad esempio istruiti in merito al rischio di aprire un malware.

ART. 2 OPDa | OBIETTIVI

Il titolare e il responsabile del trattamento **adottano provvedimenti tecnici e organizzativi** affinché i dati trattati:

A

Siano accessibili solo alle persone autorizzate (**confidenzialità**)

B

Siano disponibili quando necessario (**disponibilità**)

C

Non siano modificati indebitamente o inavvertitamente (**integrità**)

D

Siano trattati in modo tracciabile (**tracciabilità**)

ART. 3 OPDa | PROVVEDIMENTI TECNICI E ORGANIZZATIVI

Cosa devono garantire i provvedimenti adottati? Alcuni esempi:

a. Che le persone autorizzate abbiano accesso solo ai dati personali di cui abbisognano al fine di adempiere i loro compiti (**controllo dell'accesso ai dati**);

b. Che solo le persone autorizzate abbiano accesso ai locali e agli impianti utilizzati per il trattamento dei dati personali (**controllo dell'accesso ai locali e agli impianti**);

c. Che le persone non autorizzate non possano utilizzare i sistemi di trattamento automatizzato di dati personali con l'ausilio di impianti di trasmissione (**controllo degli utenti**).

[…]

E

DATA BREACH

DATA BREACH | I VARI TIPI DI VIOLAZIONE

"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"

"***Violazione della riservatezza***", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali

"***Violazione dell'integrità***", in caso di modifica non autorizzata o accidentale dei dati personali

"***Violazione della disponibilità***", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali

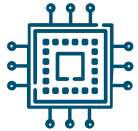
DATA BREACH | ALCUNI ESEMPI

Perdita o furto di device mobili non criptati (usb, laptop, smartphone) che contengono dati personali

Invio di un file/email contenente dati personali al **destinatario errato**

Invio di una email massiva a una **lista di contatti nel campo "a:" o "cc:"** invece che in "**ccn**:"

Perdita o furto di documenti cartacei contenenti dati personali



Attacchi informatici (malware, virus, criptolocker etc.) a sistemi contenenti dati personali

Dati sanitari | cartelle cliniche **indisponibili** per alcune ore a causa di attacco informatico o distacco elettrico

DATA BREACH | L'IMPORTANZA DELLA GESTIONE INTERNA

RUOLI E RESPONSABILITA'

(referente privacy? IT?)

PROCEDURE / DIRETTIVE PER LA GESTIONE DELLE VIOLAZIONE

REPORTING INTERNO ED ESTERNO

(canale e-mail dedicato?)

ACCORDI CON I RESPONSABILI ESTERNI

(clausole contrattuali specifiche su Data breach)

PIANI DI INTERVENTO

(piano di rimedio e adozione di misure di sicurezza)

DATA BREACH | NOTIFICA

Art. 24 LPD | Notifica di violazioni della sicurezza dei dati

Il titolare del trattamento notifica **quanto prima** all'IFPDT ogni violazione della sicurezza dei dati che comporta verosimilmente un **rischio elevato** per la personalità o i diritti fondamentali della persona interessata.

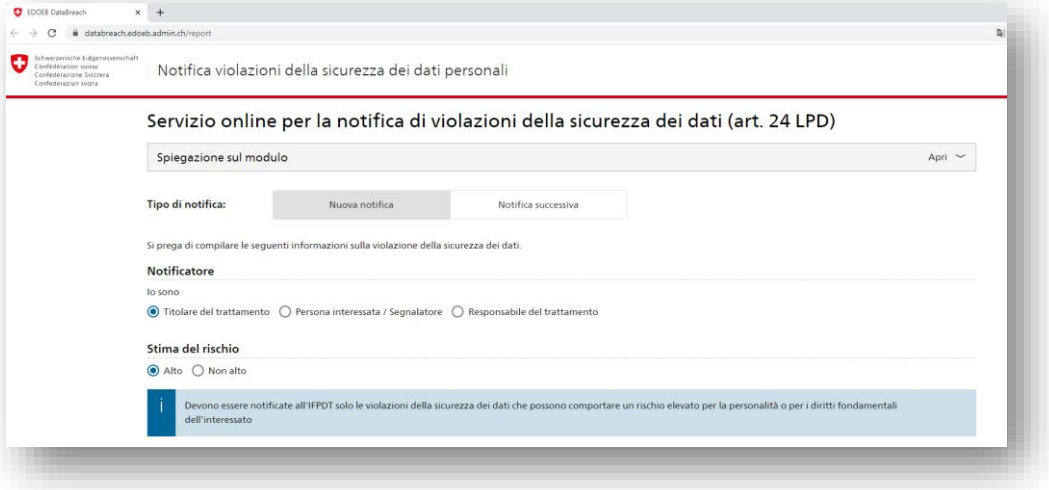
Nella notifica il titolare del trattamento menziona **almeno il tipo di violazione della sicurezza dei dati, le sue conseguenze e le misure disposte o previste**.

Il responsabile del trattamento informa quanto prima il titolare del trattamento su ogni violazione della sicurezza dei dati.

DATA BREACH | COME SI NOTIFICHERA' ALL'IFPDT

LA PROCEDURA TELEMATICA DI NOTIFICA

(link: https://databreach.edoeb.admin.ch/report)



DATA BREACH | COMUNICAZIONE AGLI INTERESSATI

Il titolare del trattamento informa la persona interessata sulla violazione della sicurezza dei dati, se ciò è necessario per proteggere la persona interessata o se lo esige l'IFPDT.

Il titolare del trattamento può limitare o differire l'informazione della persona interessata o rinunciarvi se: a. sussiste uno dei motivi di cui all'articolo 26 capoversi 1 lettera b o 2 lettera b oppure un obbligo legale di serbare il segreto; b. l'informazione è impossibile o richiede un onere sproporzionato; o c. l'informazione è garantita in modo equivalente con una comunicazione pubblica.

Una notifica effettuata in forza del presente articolo può essere usata nel quadro di un procedimento penale contro la persona soggetta all'obbligo di notifica soltanto con il suo consenso.

F

VIDEOSORVEGLIANZA

VIDEOSORVEGLIANZA

VIDEOSORVEGLIANZA DA PARTE DI PERSONE PRIVATE

VIDEVIDEOSORVEGLIANZA SUL POSTO DI LAVORO

VIDEOSORVEGLIANZA DA PARTE DI PERSONE PRIVATE | SVIZZERA

L'installazione di un impianto di videosorveglianza comporta l'elaborazione continua di dati personali.

Rischio → **ingerenza nella sfera privata delle persone riprese**

Importanza della LPD, legge sulla protezione dei dati personali nelle diverse fasi:

- *DEFINIZIONE*
- *INSTALLAZIONE*
- *UTILIZZO*

VIDEOSORVEGLIANZA DA PARTE DI PERSONE PRIVATE | SVIZZERA

SUPSI

Liceità

La lesione della personalità è giustificata dal consenso dell'interessato, da un interesse preponderante pubblico o privato o da una legge.

Proporzionalità

Adeguatezza del mezzo rispetto all'obbiettivo fissato, ossia ad esempio, la sicurezza, la protezione delle cose e/o delle persone.

Rapporto ragionevole e bilanciato

Tra l'ingerenza nella sfera privata e lo scopo perseguito

- Buona fede
- Trasparenza

VIDEOSORVEGLIANZA DA PARTE DI PERSONE PRIVATE

Sicurezza dei dati – adozione di provvedimenti tecnici e organizzativi per proteggere i dati personali

Esempi:

1. Conservazione in luogo sicuro e chiuso a chiave con accesso ad opera delle sole persone autorizzate

2. In caso di trasmissione delle immagini utilizzo di canali cifrati o misure atte ad impedire che persone autorizzate possano osservare i dati

3. Limitazione del numero di persone che possono accedere alle immagini (live o registrate)

4

Monitor collocati in modo tale da consentirne la visione soltanto ad opera di soggetti autorizzati - No monitor accessibili al pubblico

5

I dati non devono essere comunicati a terzi a meno che le immagini non vengano consegnate alle autorità preposte al perseguimento penale al fine di sporgere denuncia o casi previsti/consentiti dalla legge es. richiesta del giudice

6

Cancellazione delle immagini in breve tempo.

Individuazione di danni a persone o cose in breve tempo -> 24 ore tempo sufficiente

7

Ragioni di conservazione più lunghe, proroga dei tempi di conservazione.

VIDEOSORVEGLIANZA E LUOGHI DI LAVORO

Controlli più invasivi legittimi solo a fronte della rilevazione di specifiche anomalie e all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori.

Telecamere: autorizzabile da **postazione remota** sia la visione delle immagini "in tempo reale" che registrate.

Necessaria **gradualità nell'ampiezza e tipologia del monitoraggio** secondo principi di legittimità e determinatezza del fine perseguito, nonché della sua proporzionalità, correttezza e non eccedenza.

VIDEOSORVEGLIANZA SUL POSTO DI LAVORO

Art. 31 LPD Motivi giustificativi

«1. Una lesione della personalità è illecita se non è giustificata dal consenso della persona interessata, da un interesse preponderante privato o pubblico oppure dalla legge»

Il consenso espresso nell'ambito del rapporto di lavoro ha una valenza limitata. La libera volontà dei collaboratori è condizionata dal rapporto di subordinazione. I lavoratori, o i loro rappresentanti, hanno inoltre il diritto di essere consultati e devono essere informati prima dell'installazione di un impianto di videosorveglianza

OBBLIGO DI INFORMARE FONDATO SUL PRINCIPIO DELLA TRASPARENZA

VIDEOSORVEGLIANZA SUL POSTO DI LAVORO

«L'esperienza insegna che gli impianti di videosorveglianza provocano sentimenti negativi nei lavoratori interessati e deteriorano l'ambiente di lavoro in generale.

Possono pregiudicare il benessere fisico e psicologico e, di conseguenza, l'efficienza del dipendente.

È dunque nell'interesse di tutte le persone coinvolte utilizzare impianti di videosorveglianza solo se non è possibile raggiungere lo scopo perseguito mediante misure meno incisive.»

VIDEOSORVEGLIANZA SUL POSTO DI LAVORO

La **sorveglianza** del comportamento che avviene **senza preavviso** (sorveglianza nascosta) **viola** inoltre il principio della buona fede (art. 4 cpv. 2 LDP). Se necessaria per altri motivi, la videosorveglianza deve essere concepita e disposta in modo da non pregiudicare la salute e la libertà di movimento dei lavoratori..

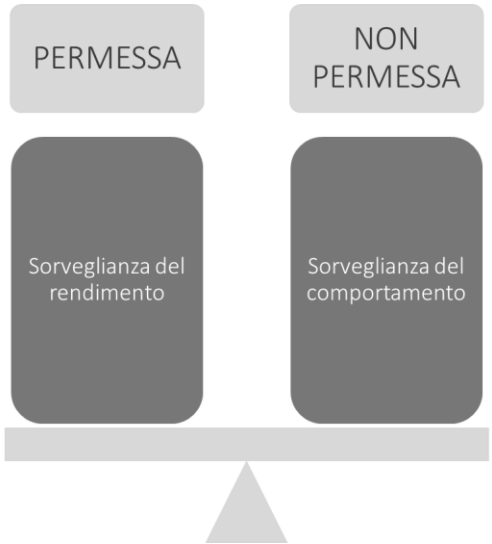
I sistemi di **videosorveglianza volti specificamente al controllo mirato del comportamento dei lavoratori** sono **vietati** poiché sono contrari a vari aspetti della protezione della personalità di cui godono questi ultimi

VIDEOSORVEGLIANZA SUL POSTO DI LAVORO

Art. 26 dell'ordinanza 3 concernente la legge sul lavoro:

1. *Non è ammessa l'applicazione di sistemi di sorveglianza e di **controllo del comportamento** dei lavoratori sul posto di lavoro*
2. *I sistemi di sorveglianza o controllo, se sono necessari per altre ragioni devono essere concepiti e disposti in modo da non pregiudicare la salute e la libertà di movimento dei lavoratori»*

VIDEOSORVEGLIANZA SUL POSTO DI LAVORO



Proporzionalità: 3 condizioni

Interesse preponderante (es. sicurezza del personale / dell'azienda / ottimizzazione della produzione)

Proporzionalità tra l'interesse del datore di lavoro alla sorveglianza l'interesse dei lavoratori a non essere sorvegliati

Partecipazione dei lavoratori

COSA DEVE FARE L'AZIENDA?

1. Valutare l'interesse preponderante
2. Valutare la proporzionalità tra mezzi e interessi
3. Preparare un documento che spieghi la logica del sistema
4. Informare i collaboratori – discussione / interlocuzione con il personale / consultare la rappresentanza dei lavoratori in azienda
5. Elaborare un regolamento interno che contenga informazioni trasparenti per i lavoratori in merito ai loro diritti e doveri

VIDEOSORVEGLIANZA | OBBLIGHI DEL TITOLARE

I dipendenti incaricati devono essere nominati ***soggetti autorizzati*** al trattamento delle immagini. In questo modo il titolare garantisce diversi livelli di visibilità e trattamento delle immagini per tutti i soggetti autorizzati, limitando la possibilità di visione:

- **Live**
- **Registrate** (tenendo traccia dei file di Log degli accessi dei soggetti interni ed esterni)

VIDEOSORVEGLIANZA | OBBLIGHI DEL TITOLARE

Configurazione del sistema

Ottenere dall'installatore la dichiarazione di **conformità privacy** dell'impianto che garantisca la possibilità di impostare:

- **Credenziali di autenticazione**

  Utilizzo di User ID / password per ciascun autorizzato alla visione delle immagini.

- **Cambio Password**

  Reimpostazione al primo utilizzo, password adeguata (es. caratteri speciali e lunghezza) e con scadenza automatica periodica.

- **Cancellazione automatica delle immagini (se registrate)**

  Da configurare allo scadere del tempo di conservazione stabilito, con possibilità di calendarizzazione dei giorni di chiusura.

VIDEOSORVEGLIANZA | OBBLIGHI DEL TITOLARE

- **Crittografia**

  Da adottare in caso di trasmissione/comunicazione immagini esterna (VPN / HTTPS).

- **Access Log degli ADS e degli utenti autorizzati alla visione del registrato (da conservare per almeno 6 mesi)**

  I log devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica dell'integrità.

- **Accesso, cancellazione, limitazione di trattamento**

  Introduzione di sistemi / procedure atti a gestire l'esercizio dei diritti da parte dell'interessato.

- **Misure organizzative e misure tecniche**

  Il sistema deve garantire la possibilità di introdurre adeguate misure di sicurezza.

VIDEOSORVEGLIANZA | INSTALLAZIONE

Assistenza e manutenzione

Il Titolare del trattamento, sulla base delle attività svolte dai soggetti che si occupano dell'installazione e/o assistenza e manutenzione dell'impianto di videosorveglianza, dovrà valutare la nomina a **responsabile del trattamento**.

VIDEOSORVEGLIANZA | TEMPI DI CONSERVAZIONE

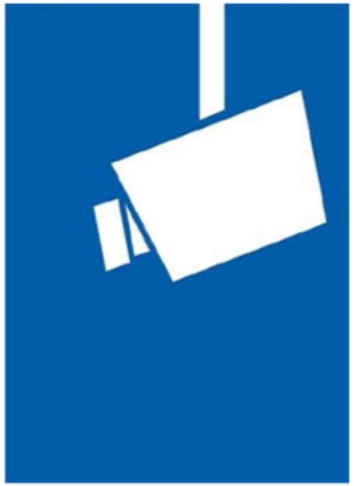
Principio di proporzionalità: le immagini possano essere conservate solo per il tempo strettamente necessario al perseguimento della finalità prefissata.

Andranno predisposte misure tecniche od organizzative per la **cancellazione, anche in forma automatica**, delle registrazioni, allo scadere del termine di legge: sovrascrittura, cancellazione.

Tocca al singolo titolare del trattamento determinare, **caso per caso**, quanto a lungo sia lecito protrarre un trattamento di dati personali, nel rispetto dei diversi principi cui si ispira la disciplina europea, ossia **72 ore**, salvo che specifiche norme di legge non prevedano espressamente determinati tempi di conservazione dei dati.

In ogni caso, rispetto alla specifica finalità perseguita, "*Quanto più prolungato è il periodo di conservazione previsto, tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione*."

INFORMATIVA PRIVACY – PRIMO LIVELLO



Videosorveglianza!

Informativa sul trattamento di dati personali

Titolare del trattamento: [redacted], **Titolare del trattamento**, con sede legale in [redacted]

Modalità di trattamento e conservazione dei dati: L'impianto rileva e registra le immagini in tempo reale. Il Titolare conserva le immagini per **x giorni** con successiva cancellazione automatica.

Finalità del trattamento: La sicurezza e tutela del patrimonio aziendale e delle persone fisiche.

Diritti dell'interessato: L'interessato potrà far valere i propri diritti (tra cui ad esempio il diritto di accesso), scrivendo al Titolare a info@[redacted] o al CPD I DPO all'indirizzo dpo@[redacted]

Maggiori informazioni sul trattamento e sui diritti dell'interessato sono disponibili all'interno dell'informativa estesa reperibile:
- in forma cartacea presso la reception di [redacted]
- scansionando il QR Code a lato;
- all'indirizzo e-mail info@[redacted]

INFORMATIVA PRIVACY – SECONDO LIVELLO

INFORMATIVA DI SECONDO LIVELLO

Informativa dipendenti e Informativa visitatori/clienti

Devono essere rese disponibili in un **luogo facilmente accessibile** agli interessati (es. reception o sito dell'organizzazione).

In ogni caso, ***deve essere possibile accedere alle informazioni di secondo livello senza accedere all'area videosorvegliata***.

G

SITO INTERNET E COOKIES

SITO INTERNET E COOKIES

Avviene un trattamento di dati attraverso un sito internet? Il sito rilascia cookies? Di che tipo? Quali sono questi dati?

- Indirizzi IP
- Nomi, cognomi, dati di contatto
- Immagini
- Preferenze, abitudini di consumo

Per quali finalità / scopi vengono trattati?

- Navigazione sul sito;
- Analisi statistica di vario genere (miglioramento della performance del sito, profilazione dell'utente);
- richieste di contatto; newsletter;
- raccolta di CV;
- vendita di prodotti.

IMPORTANTE

Il **sito internet** è la **vetrina della società!**

COSA SONO I COOKIES?

Qual è la definizione di «cookie»?

I **cookie** (“biscotto” in inglese) sono dei piccoli file di testo necessari affinché il server del sito web che li ha installati possa ottenere informazioni sulla specifica attività che l’utente compie su quelle determinate pagine web.

A cosa servono?

Esempio: Chi si è collegato a quel sito e che cosa ha fatto.

Come funzionano?

Ogni volta che il dispositivo dell’utente si ricollega al sito, lo stesso gli rimanda il cookie al fine di riconoscere e tracciare l’attività dell’utente anche a distanza di tempo.

LE CATEGORIE DI COOKIES

COOKIE TECNICI

COOKIE SESSIONE

Possono essere temporanei e cancellarsi al termine della singola sessione.

COOKIE PERMANENTI

Possono rimanere “nascosti” nei meandri delle cartelle del nostro pc, rientrando in collegamento con l’applicazione web ogni volta che l’utente si riconnette al medesimo server remoto.

LE CATEGORIE DI COOKIES

COOKIE DI PROFILAZIONE

- Consentono di “profilare” l’utente perché il sito grazie a questi file può ricostruire tutte le attività fatte da quel browser e dispositivo nel tempo.
- Monitorano il comportamento e le preferenze di navigazione dell’utente costruendo profili dettagliati in base alle loro attività online.

SITO INTERNET E COOKIES

Come procedere?

I. Analisi del sito web della società

1. Ubicazione del sito (hosting del sito web):
   - Svizzera?
   - Fuori dal territorio della Confederazione?
   - Fuori dal territorio della Confederazione e fuori da SEE?

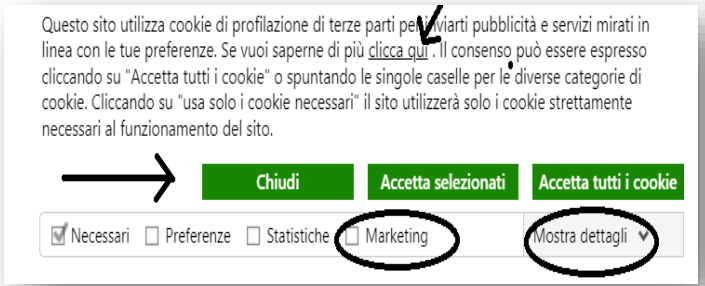
2. Mappatura dei fornitori che supporto il Titolare per assistenza/manutenzione del sito web:
   - Chi è il fornitore dell'hosting?
   - Chi è il fornitore per attività di manutenzione/assistenza?
   - Chi è il fornitore per la parte di analisi e SEO?

SITO INTERNET E COOKIES

3. Quali sono le finalità per vengono trattati i dati raccolti attraverso il sito web?
4. Analisi dei cookies (tecnici? Di Profilazione?)
5. Vi sono dei form dove gli utenti possono inserire dati e inviarli all'azienda?

II. Predisposizione dei principali documenti per la conformità del sito internet

1. Banner cookies (informativa breve) e caratteristiche:
   - scelta per specifiche categorie di cookies;
   - Pulsanti di opzione:



«Accetta tutti i cookies» «Rifiuta tutti i cookies»
«X» o «pulsante che faccia scomparire il banner»

SITO INTERNET E COOKIES

2. Stesura dell'**informativa privacy sui cookie** (informativa estesa) che descrive nel dettaglio i trattamenti di dati effettuati tramite tali strumenti (i cookie appunto).

COOKIE POLICY

Informativa estesa sui cookie

Cookie utilizzati da Privacy Desk Suisse. Questo sito utilizza cookie di profilazione di terze parti per inviarti pubblicità e servizi mirati in linea con le tue preferenze. Se vuoi saperne di più clicca qui . Il consenso può essere espresso cliccando su "Accetta tutti i cookie" o spuntando le singole caselle per le diverse categorie di cookie. Cliccando su "usa solo i cookie necessari" il sito utilizzerà solo i cookie strettamente necessari al funzionamento del sito.

Cosa sono i cookies

I cookie sono piccoli file di testo che i siti visitati dagli utenti inviano ai loro terminali, dove vengono memorizzati per essere ritrasmessi agli stessi siti nelle visite successive.

I cookie vengono utilizzati per scopi diversi, hanno caratteristiche diverse, e possono essere utilizzati sia dal titolare del trattamento dei dati del sito che si sta visitando, sia da terzi.

Di seguito troverete tutte le informazioni sui cookie installati attraverso questo sito, e le informazioni necessarie su come gestire le vostre preferenze riguardo ad essi.

Per maggiori informazioni sui cookie e sulle loro funzioni generali, visita un sito informativo come https://www.allaboutcookies.org/.

SITO INTERNET E COOKIES

3. Stesura dell'**informativa privacy generale** che descrive nel dettaglio i trattamenti di dati effettuati attraverso il sito (es. raccolta dati nei form di contatto/richieste di preventivo, iscrizione a newsletter)

PRIVACY NOTICE

Documento informativo sui trattamenti di dati personali

Nel rispetto di quanto previsto dalla Legge federale sulla protezione dei dati (LPD). Le forniamo le dovute informazioni in ordine al trattamento dei dati personali forniti nel corso della navigazione sul presente sito internet. L'informativa non è da considerarsi valida per altri siti web (ad esempio altri siti consultabili tramite links di collegamento presenti sulla presente pagina), che non è da considerarsi in alcun modo responsabile dei siti internet di terzi soggetti.

Quali sono i dati personali trattati? Cosa significa trattamento? chi è l'interessato?

Dato personale: qualsiasi informazione riguardante un interessato che lo identifichi o lo renda identificabile. Privacy Desk Suisse SA, attraverso il sito web, raccoglie diversi dati personali, a titolo esemplificativo non esaustivo: nome, cognome, indirizzo e-mail, numero di telefono, indirizzo IP.
Trattamento è qualunque operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, e applicate a dati personali o insieme 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.
Interessato è la persona fisica indentificata o identificabile. A titolo esemplificativo (non esaustivo), interessato è l'utente che naviga sulla piattaforma e che invia, per il tramite della stessa, una richiesta di informazioni.

GRAZIE DELL'ATTENZIONE