TRATTAMENTO DEI DATI PERSONALI
ISTRUZIONI SULLA SICUREZZA

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

Alla luce delle attività di verifica svolte, considerato il livello di rischio rilevato in relazione alle attività svolte, analizzati l'oggetto, il contesto e le finalità del trattamento perseguite nonché gli strumenti utilizzati, al fine di garantire un livello di sicurezza adeguato, si consiglia l'adozione immediata ed il mantenimento costante delle seguenti misure di sicurezza:

1) MISURE DI SICUREZZA

a. Organizzative

- ☐ Verificare con cadenza quantomeno annuale che le autorizzazioni fornite ai dipendenti e i servizi svolti dai responsabili esterni siano ancora attuali e rispondenti a quanto stabilito in sede di definizione del rapporto;
- ☐ Controllo accessi archivio
- ☐ Divieto di utilizzo dei supporti removibili
- ☐ Formazione del personale
- ☐ In caso di assunzione di nuovi dipendenti, di nuove collaborazioni con ulteriori soggetti esterni, ovvero di variazione delle mansioni definite in sede di sottoscrizione dell'accordo, comunicarlo al Vs Consulente Privacy in modo tale da aggiornare la relativa documentazione
- ☐ Istruzioni per utilizzo della posta elettronica
- ☐ Manutenzione periodica apparecchiature
- ☐ Minimizzazione dei dati
- ☐ Monitoraggio autorizzazioni (cancellazione/modifica credenziali di accesso)
- ☐ Monitoraggio tempi conservazione dati e cancellazione
- ☐ Procedure di archiviazione dati e download
- ☐ Procedure di archiviazione e gestione consensi
- ☐ Procedure gestione delle postazioni di lavoro (workstation)
- ☐ Procedure per la gestione, custodia, uso e smaltimento dei supporti removibili
- ☐ Procedure per la gestione dei documenti cartacei
- ☐ Procedure per la gestione delle credenziali
- ☐ Procedure per la gestione delle richieste di informazioni degli interessati e relativa identificazione
- ☐ Procedure per lo smaltimento degli archivi
- ☐ Protocollo gestione incidenti di sicurezza e violazioni dei dati
- ☐ Registrazione accessi

b. Fisiche

- ☐ Archivi separati con accesso limitato
- ☐ Archivi dotati di serratura in tutti i locali contenenti fisicamente dati
- ☐ Controllo degli accessi fisici
- ☐ Impianto di climatizzazione

- ☐ Impianto elettrico dotato di misure salvavita atte anche a evitare cortocircuiti e possibili incendi
- ☐ Impianto elettrico è certificato e a norma
- ☐ Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- ☐ Protezione dei locali con serrature di sicurezza e porte blindate
- ☐ Sistema di allarme
- ☐ Sistemi antincendio
- ☐ Tritadocumenti

c. Tecniche

- ☐ Accesso da remoto su rete aziendale sicuro
- ☐ Anonimizzazione dei dati
- ☐ Programma antivirus idoneo all'utilizzo professionale
- ☐ Architettura di rete sicura:
    - Segmentazione
    - Server separati
    - Ridondanza
    - Singoli punti di errore
    - Crittografia: ☐ E2E ☐ P2P
    - DMZ
- ☐ Autenticazione in più fattori
- ☐ Backup dei dati periodico
- ☐ Blocco accesso siti indesiderati (URL Filtering)
- ☐ Archiviazione dei log di sistema
- ☐ Archiviazione e gestione automatizzata consensi
- ☐ Cancellazione automatizzata dei dati (tempi di conservazione)
- ☐ Controllo degli accessi tramite un Identity Provider
- ☐ Crittografia dei dati
- ☐ Data center certificato ISO 9001, ISO 14001, ISO 27001
- ☐ Firewall idoneo all'utilizzo professionale
- ☐ Gruppo di continuità/stabilizzatore
- ☐ Identificazione utenti
- ☐ Intrusion Detection System (IDS)
- ☐ Livelli di accesso ai database differenziati
- ☐ Livelli di accesso alle immagini differenziati
- ☐ Partizionamento dei dischi di sistema
- ☐ Password costituita da almeno 8 caratteri alfanumerici e caratteri speciali
- ☐ Password modificate al primo utilizzo
- ☐ Password modificate ogni 3/6 mesi
- ☐ Cambio password automatizzato
- ☐ Procedure di Disaster Recovery e Business Continuity
- ☐ Protocollo di rete SSL

- ☐ Registrazione accessi
- ☐ Sicurezza delle postazioni di lavoro
  - Gli utenti non sono in grado di disattivare o bypassare le impostazioni di sicurezza
  - Le applicazioni anti-virus sono aggiornate regolarmente
  - Gli utenti non hanno i privilegi per installare o disattivare applicazioni software non autorizzate
  - Il sistema attiva il timeout di sessione quando l'utente non è stato attivo per ...
  - Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo sono installati regolarmente
  - È prevista una politica relativa al salvataggio dei file contenenti dati
  - È prevista una politica relativa ai download dei file contenenti dati
- ☐ Utilizzo chiavette USB e altri supporti removibili
  - Non consentito/bloccato
  - Consentito solo a dispositivi pre-registrati e pre-autorizzati
  - Consentito a dispositivi dotati di credenziali di autenticazione
  - Consentito a dispositivi dotati di sistemi di cifratura
- ☐ VDS
- ☐ VPN
- ☐ E-mail provider che offra garanzie adeguate in merito alla protezione dei dati personali

2) MISURE RELATIVE ALL'IMPIANTO DI VIDEOSORVEGLIANZA

- ☐ Predisporre un elenco di tutte le telecamere presenti presso la sede del titolare, indicando: le funzionalità (monitoraggio in tempo reale o registrazione), la localizzazione, eventuali specifiche di configurazione (es. per quante ore è accesa, se si attiva solo al movimento delle persone, ecc.) e il supporto di registrazione su cui le immagini vengono memorizzate
- ☐ Affiggere in un luogo ben visibile l'informativa sintetica relativa alla videosorveglianza
- ☐ Provvedere ad aggiornare la cartellonistica relativa alla videosorveglianza
- ☐ Limitare la durata della registrazione del sistema di videosorveglianza a quanto prescritto dalla normativa ed indicato nell'eventuale provvedimento di autorizzazione dell'impianto. Decorso tale periodo i filmati dovranno essere cancellati (si consiglia, avvalendosi della consulenza del tecnico competente, di predisporre un sistema di cancellazione automatico delle registrazioni)

3) MISURE INFORMATICHE RELATIVE AL SITO INTERNET

- ☐ Inserire nel *footer* del sito il riferimento e il link alla Privacy Policy ed alla Cookie Policy.
  In relazione alla Cookie Policy si ricorda che:
  - Deve essere costantemente aggiornata, così da rispecchiare i cookie realmente utilizzati
  - Deve essere presente un banner all'apertura del sito riportante l'indicazione dei cookie utilizzati ed il pannello di gestione degli stessi (o il link al pannello di gestione)
  - L'interessato deve poter scegliere quali cookie accettare (con particolare riferimento ai cookie aventi finalità di marketing e profilazione)
- ☐ Implementare il protocollo HTTPS (*Hypertext Transfer Protocol Secure*) in ogni sezione del sito web per garantire livelli più cautelativi dell'integrità e della riservatezza del dato

In merito ad una corretta gestione ed impostazione delle pagine web aziendali, si ricorda inoltre che:

- In caso di eventuale richiesta di CONSENSO al trattamento, questo deve essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesti l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano. A tal proposito, azioni come lo *scrolling* o lo *swiping* di una pagina Web non soddisfano il requisito di "azione chiara e inequivocabile".
  In merito alle modalità di acquisizione del consenso *on-line* si precisa altresì che:
  - il consenso rilasciato deve essere tracciato e comprovabile, ad esempio mediante la creazione di *log file*
  - affinché il consenso sia prestato liberamente, l'accesso ai servizi e alle funzionalità del sito non deve essere subordinato alla dazione del consenso di un utente alla memorizzazione delle informazioni o all'ottenimento delle informazioni già memorizzate nel terminale (divieto del c.d. *cookie wall*)

  Il consenso, una volta correttamente acquisito, non dovrà essere nuovamente richiesto se non all'eventuale mutare di una o più delle condizioni alle quali è stato raccolto ovvero quando sia impossibile avere contezza del fatto che un cookie sia stato già in precedenza memorizzato sul dispositivo.
  Si ricorda, inoltre, che:
  - nel caso di raccolta del consenso/presa visione per mezzo di un *checkbox*, la casella di spunta non deve essere preselezionata e deve essere presente una dicitura similare a: "*Ho preso visione della Privacy Policy e desidero iscrivermi al servizio*" con link alla privacy policy del sito.
  - nessuna tecnica di profilazione, di natura sia attiva sia passiva, deve essere attuata per impostazione predefinita al momento del primo accesso dell'Utente al sito web
  - i cookie cd. *analytics* - affinché siano ricompresi nella categoria dei cookie tecnici e come tali essere utilizzati in assenza della previa acquisizione del consenso dell'interessato - devono essere impostati in modo tale da precludere la possibilità che si pervenga, mediante il loro utilizzo, alla diretta individuazione dell'interessato (cd. *single out*)
- COOKIE E IDENTIFICATORI NON TECNICI
  Se si trattano cookie e altri identificatori "non tecnici", si può utilizzare un banner a comparsa immediata e di adeguate dimensioni che contenga:
  a. l'indicazione che il sito utilizza cookie tecnici e, previo consenso dell'utente, cookie di profilazione o altri strumenti di tracciamento indicando le relative finalità (informativa breve);
  b. il link alla privacy policy contenente l'informativa completa, inclusi gli eventuali altri soggetti destinatari dei dati personali, i tempi di conservazione dei dati e l'esercizio dei diritti di cui al Regolamento;
  c. l'avvertenza che la chiusura del banner (ad es. mediante selezione dell'apposito comando contraddistinto dalla X posta al suo interno, in alto a destra) comporta il permanere delle impostazioni di default e dunque la continuazione della navigazione in assenza di cookie o altri strumenti di tracciamento diversi da quelli tecnici.

  Ai fini dell'acquisizione del consenso, il banner dovrà contenere:
  a. il menzionato comando (es. una X in alto a destra) per chiudere il banner senza prestare il consenso all'uso dei cookie o delle altre tecniche di profilazione mantenendo le impostazioni di default;
  b. un comando per accettare tutti i cookie o altre tecniche di tracciamento;

c. il link ad un'altra area nella quale poter scegliere in modo analitico le funzionalità, le terze parti e i cookie che si vogliono installare e poter prestare il consenso all'impiego di tutti i cookie se non dato in precedenza o revocarlo, anche in unica soluzione, se già espresso.

Al riguardo, è buona prassi l'impiego di un segno grafico, una icona o altro accorgimento tecnico che indichi, anche in modo essenziale, ad es. nel *footer* di ogni pagina del dominio, lo stato dei consensi in precedenza resi dall'utente consentendone l'eventuale modifica o aggiornamento.

Tale area dedicata alle scelte di dettaglio dovrà essere raggiungibile anche tramite un ulteriore link posizionato nel *footer* di qualsiasi pagina del dominio.

4) FIRMA DELL'E-MAIL/PEC/FAX:

Inserire nella firma dell'e-mail/PEC/fax la seguente dicitura:

"Le informazioni, i dati e le notizie contenute nella presente comunicazione e i relativi allegati sono di natura privata e come tali possono essere riservate e sono, comunque, destinate esclusivamente ai destinatari indicati in epigrafe. La diffusione, distribuzione e/o la copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 c.p., sia ai sensi del d.lgs. n. 196/2003 e del Regolamento (UE) 2016/679. Se avete ricevuto questo messaggio per errore, Vi preghiamo di distruggerlo e di darcene immediata comunicazione anche inviando un messaggio di ritorno all'indirizzo e-mail del mittente. Grazie!
This e-mail (including attachments) is intended only for the recipient(s) named above. It may contain confidential or privileged information and should not be read, copied or otherwise used by any other person. If you are not the named recipient, please contact us and delete the e-mail from your system. Thanks! (Rif. d.lgs. 196/2003 and Regulation (EU) 2016/679)"

5) ADEGUAMENTO CLAUSOLA CONTRATTUALE

Tutela dei dati personali
Le parti dichiarano che i dati personali forniti per le finalità di cui al presente contratto saranno trattati nel rispetto delle disposizioni previste dal Regolamento (UE) 2016/679 (GDPR) e dalla normativa nazionale vigente in materia. In particolare, saranno trattati in modo lecito, corretto, trasparente e raccolti per finalità determinate, esplicite e legittime. Sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Versione 2: Clausola estesa

Tutela dei dati personali
I dati personali conferiti dall'Interessato sono trattati nel rispetto delle disposizioni previste dal Regolamento (UE) 2016/679 (GDPR) e dalla normativa nazionale vigente in materia. In particolare, sono trattati in modo lecito, corretto e trasparente; raccolti per finalità determinate, esplicite e legittime; sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati; sono esatti e, se necessario, aggiornati; conservati in una forma che consente l'identificazione dell' Interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; trattati in modo da garantire un'adeguata sicurezza, compresa la protezione

mediante misure tecniche e organizzative adeguate. L'Interessato con la sottoscrizione del presente contratto dichiara di aver ricevuto le informazioni relative alla tutela e alla protezione dei propri dati personali rese ai sensi degli artt.13 e 14 del GDPR e della normativa nazionale vigente in materia, allegate al presente contratto, costituendone parte integrante e sostanziale dello stesso.