swissstaffing

Nota Informativa: Legge federale rivista sulla protezione dei dati (nLPD)

Conseguenze per i prestatori di personale in Svizzera

1. Situazione di partenza

Il 1° settembre 2023 entrerà in vigore la revisione totale della legge federale sulla protezione dei dati (legge sulla protezione dei dati; nLPD) unitamente all'ordinanza sulla protezione dei dati (OPDa) e all'ordinanza sulle certificazioni in materia di protezione dei dati (OCPD). Non ci sarà un periodo di transizione.

Con l'entrata in vigore della nLPD, i prestatori di personale dovranno rispettare nuovi obblighi e adottare i relativi provvedimenti. Pertanto, di seguito si intende descrivere questi ultimi più nel dettaglio. I riferimenti alle rispettive disposizioni di legge si riferiscono alla LPD rivista (nLPD).

La nLPD ha lo scopo di proteggere la personalità e i diritti fondamentali delle persone in merito alle quali vengono trattati dati personali (di seguito denominati anche «dati») (art. 1 nLPD). Si applica al trattamento di dati personali di persone fisiche da parte di imprese private e di organi federali (art. 2 cpv. 1 nLPD).

La nLPD intende realizzare diversi obiettivi:

- le carenze dell'attuale LPD del 1992, che sono venute a crearsi a causa del rapido sviluppo tecnologico, dovranno essere colmate;
- si deve tenere conto degli sviluppi nell'Unione europea e della protezione dei dati in Svizzera per poterla allineare con il regolamento generale europeo sulla protezione dei dati (GDPR UE). Quest'ultimo è in vigore dal 25 maggio 2018 (vedi Promemoria swissstaffing del maggio 2018). [Per gli adeguamenti per le aziende che hanno già attuato i requisiti del GDPR UE, vedere l'allegato LISTA DI CONTROLLO 1: DAL GDPR UE ALL'nLPD];
- Si devono promuovere le buone pratiche aumentando gli obblighi delle persone responsabili del trattamento dei dati e rafforzando i diritti delle persone interessate dal trattamento dei dati nonché le competenze di vigilanza dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).

2. Che cosa rimane invariato con l'entrata in vigore dell'nLPD rivista?

Nell'nLPD rimangono invariati i principi di base del trattamento dei dati. Pertanto, se vengono rispettati i principi di trattamento elencati di seguito, per il trattamento dei dati personali in linea di principio non è necessario né il consenso né un motivo giustificativo (art. 6, 7 e 8 in combinato disposto con l'art. 30 nLPD):

- I dati possono essere raccolti solo legalmente. Ciò significa che non possono essere ottenuti mediante minaccia o inganno oppure senza che gli interessati ne siano al corrente (art. 6 cpv. 1 nLPD).
- Il trattamento dei dati deve essere effettuato in buona fede. Si applica quindi il principio di una condotta leale, affidabile e rispettosa (art. 6 cpv. 2 nLPD).
- Il principio di proporzionalità deve essere rispettato. Quest'ultimo stabilisce che nel singolo caso deve essere trattato il numero di dati strettamente necessario al conseguimento dell'obiettivo (art. 6 cpv. 2 e 4 nLPD).
- L'acquisizione di dati personali e in particolare lo scopo del loro trattamento devono essere riconoscibili alla persona interessata; lo scopo deve essere indicato al momento dell'acquisizione o essere visibile dalle circostanze (art. 6 cpv. 3 nLPD).

- Chi tratta dati personali deve accertarsi della loro esattezza (art. 6 cpv. 5 nLPD).
- La sicurezza dei dati deve essere garantita; ciò significa che i dati personali devono essere protetti da trattamenti non autorizzati mediante misure tecniche e organizzative adeguate (art. 8 nLPD).

Come nell'LPD precedente, si verifica una lesione della personalità quando i dati personali vengono trattati nonostante la violazione di uno dei principi generali sopra elencati o quando la persona interessata ne ha espressamente vietato il trattamento (art. 30 cpv. 1 e 2 nLPD). In questi casi il trattamento di dati personali è tuttavia consentito laddove sussista un motivo di giustificazione. I motivi di giustificazione sono il consenso della persona interessata, un interesse privato o pubblico preponderante o una legge (art. 31 cpv. 1 nLPD). L'art. 31 cpv. 2 nLPD elenca i casi in cui può sussistere un interesse privato preponderante del responsabile del trattamento (responsabile ai sensi dell'nLPD).

Oltre alle disposizioni generali dell'nLPD, il trattamento dei dati personali per il datore di lavoro in Svizzera continua a essere regolamentato come in passato anche dall'art. 328b del Codice delle obbligazioni (CO) e, per i prestatori di servizi e di personale, dalla legge sul collocamento (LC) e dall'ordinanza sul collocamento (OC). Queste disposizioni concretizzano soprattutto il principio di proporzionalità previsto dal diritto in materia di protezione dei dati (art. 6 cpv. 2 nLPD). Per il trattamento dei dati nel contesto personale si può quindi fare riferimento alle clausole già elaborate nell'ambito del GDPR UE [vedere anche ESEMPI 1: MODELLO CLAUSOLA DI CONSENSO e MODELLO 2 CLAUSOLA DI PROTEZIONE DEI DATI E DI CONSENSO IN CG allegate al presente promemoria con un modello aggiornato all'nLPD]. In particolare, devono essere osservati i seguenti punti:

- il collocatore o il prestatore di lavoro può registrare dati personali solo nella misura e per il tempo necessari per l'attività di collocamento e di prestito (art. 7 cpv. 3 e art. 18 cpv. 3 LC). Se il prestatore di personale richiede referenze sui candidati, ciò comporta il consenso della persona interessata (art. 47 cpv. 1 lett. b e art. 19 cpv. 1 lett. b OC).
- L'elaborazione di una candidatura può essere giustificata da un interesse privato preponderante del collocatore o del prestatore di lavoro al trattamento dei dati personali per l'esame della candidatura e per la trasmissione al rispettivo datore di lavoro o alla rispettiva azienda acquisitrice. La raccolta di ulteriori dati o la memorizzazione e il successivo utilizzo dei dati dei candidati dopo la conclusione della procedura di assunzione richiedono il consenso delle persone interessate a causa della finalità specifica.
- In generale, al termine della procedura di candidatura, i dati della persona interessata devono essere cancellati. Possono essere conservate solo le basi contrattuali per la fatturazione, per le quali esiste un periodo di conservazione legale di 10 anni. L'ulteriore conservazione e quindi la rinuncia alla cancellazione del fascicolo personale o la trasmissione ad altri potenziali datori di lavoro richiede il consenso della persona interessata.

In alcuni casi, per svolgere l'attività di intermediazione può essere necessario registrare dati personali degni di particolare protezione (ad esempio dati sanitari) (cfr. anche il punto 3.3 di questo promemoria). Se i dati personali degni di particolare protezione vengono comunicati dalla persona interessata insieme ai documenti di candidatura, tali dati possono essere trattati solo nell'ambito della candidatura stessa. Qualora tali dati dovessero essere riutilizzati e fosse necessario il consenso della persona interessata, questo dovrà essere fornito in forma esplicita.

swissstaffing

3. Quali sono le novità introdotte dall'nLPD?

3.1 Le persone giuridiche vengono escluse dalla tutela

Ai sensi dell'nLPD sono protetti solo i dati delle persone fisiche e non più anche quelli delle persone giuridiche, come ad esempio quelli di società anonime o di associazioni (cfr. art. 2 nLPD). Queste ultime godono della protezione prevista dal diritto societario e della protezione della personalità ai sensi del Codice civile.

3.2 Nuova terminologia: Titolare del trattamento e responsabile del trattamento

Invece di parlare, come finora, del proprietario di una collezione di dati, ora viene introdotta la coppia di termini titolare del trattamento e responsabile del trattamento. I titolari del trattamento sono imprese private (persone giuridiche) che, da sole o insieme ad altri, decidono in merito allo scopo e ai mezzi del trattamento dei dati personali (art. 5, lett. j nLPD). In caso di prestito di personale, il prestatore è titolare del trattamento, eventualmente insieme alla futura azienda acquisitrice. In qualità di datore di lavoro legale, il prestatore è il primo punto di contatto del lavoratore e tratta i dati personali per il processo di candidatura. Se si trova un'azienda acquisitrice adatta, i dati personali vengono inoltrati in modo che l'azienda acquisitrice e il prestatore elaborino in parte contemporaneamente i dati personali, di conseguenza in quel momento risultano entrambi titolari del trattamento ai sensi dell'nLPD.

A positiva conclusione di un collocamento, il datore di lavoro tratta i dati personali per i propri scopi, motivo per cui da questo momento è l'unico titolare del trattamento.

I responsabili del trattamento sono persone private, di norma anche giuridiche, che trattano dati personali per conto del titolare del trattamento (art. 5 lett. j nLPD). Esempi in merito sono il fornitore di servizi IT, al quale – sulla base della tecnologia cloud – il prestatore di personale esternalizza il trattamento dei dati, o i fornitori di servizi che elaborano le buste paga dei dipendenti del prestatore di personale.

3.3 Ampliamento del catalogo dei dati personali degni di particolare protezione

Il catalogo dei dati personali degni di particolare protezione (ad es. dati sanitari, dati politici) è stato ampliato con dati biometrici e genetici (art. 5 lett. c nLPD). Per il trattamento di dati personali degni di particolare protezione valgono requisiti più severi rispetto al trattamento di dati personali «normali». Se per il loro trattamento è necessario il consenso dell'interessato, questo deve essere fornito espressamente (art. 6 cpv. 7 lett. a nLPD).

3.4 Profilazione e profilazione ad alto rischio

Oggi lo sviluppo tecnologico consente, in misura sempre maggiore, di acquisire, elaborare, combinare e analizzare in modo automatizzato enormi quantità di dati, in modo da poter identificare, ad esempio, tendenze, correlazioni o altre caratteristiche che a loro volta possono essere attribuite a determinati gruppi. Con l'aiuto di tali gruppi di confronto, è possibile determinare o prevedere le caratteristiche o il comportamento delle singole persone fisiche, quindi ora nell'nLPD viene introdotto il concetto di profilazione. Si compie una distinzione tra profilazione «normale» e profilazione ad alto rischio. La profilazione (normale) è qualsiasi tipo di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti relativi alle prestazioni lavorative, alla situazione economica, alla salute, alle preferenze personali, agli interessi, all'affidabilità, al comportamento, alla localizzazione o agli spostamenti di tale persona fisica

(art. 5 lett. f nLPD). Tale profilazione normale si svolge, ad esempio, quando un venditore scrive a tutti gli acquirenti di determinati vini, perché ritiene molto probabile che siano interessati a una nuova fornitura di tali vini. L'nLPD non limita tale comportamento né più né meno di qualsiasi altro trattamento dei dati.

Se la profilazione comporta una correlazione di dati che consente di valutare aspetti essenziali della personalità di una persona fisica, in questo caso si tratta di una profilazione ad alto rischio. Tale trattamento comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata. Esempi applicativi includono il controllo della solvibilità e l'analisi delle frodi. In futuro, tali trattamenti potrebbero svolgere un ruolo sempre più importante anche nei processi di candidatura. In caso di profilazione ad alto rischio si applicano condizioni più severe per quanto riguarda il trattamento dei dati personali. Se è necessario il consenso della persona interessata, questo deve essere fornito espressamente (art. 6 cpv. 7 lett. b nLPD). Di norma deve essere effettuata anche una cosiddetta valutazione d'impatto sulla protezione dei dati (DPIA) (cfr. punto 3.11).

3.5 Data Protection by Design e Data Protection by Default

Secondo il principio del Data Protection by Design (protezione dei dati sin dalla progettazione) introdotto nell'nLPD, il titolare del trattamento è tenuto, nella pianificazione del trattamento dei dati, a configurarlo sul piano tecnico e organizzativo in modo tale da rispettare le norme sulla protezione dei dati (art. 7 cpv. 1 e 2 nLPD). In altre parole, un software e un hardware devono essere concepiti e sviluppati fin dall'inizio in modo da rispettare i principi del trattamento (cfr. punto 2 sopra). Inoltre, secondo il principio del Data Protection by Default (protezione dei dati per impostazione predefinita), il titolare del trattamento deve garantire, mediante impostazioni predefinite adeguate, che il trattamento dei dati personali sia limitato al minimo necessario per lo scopo d'uso, a meno che la persona interessata non disponga diversamente (art. 7 cpv. 3 nLPD).

3.6 Obbligo di informazione capillare

Secondo nLPD, le informazioni sul trattamento dei dati personali devono essere messe a disposizione delle persone interessate in modo capillare (art. 19 segg. nLPD). Le dichiarazioni sulla protezione dei dati su siti web, app e moduli sono esempi di come vengono trattati concretamente i dati personali e di come le informazioni possono essere messe a disposizione delle persone interessate. Devono essere messe a disposizione degli interessati almeno le seguenti informazioni:

- l'identità e i dati di contatto del titolare del trattamento;
- lo scopo del trattamento;
- le categorie di dati personali trattati (se non sono raccolti direttamente presso la persona);
- se del caso, i destinatari o le categorie di destinatari ai quali vengono comunicati dati personali; e
- i Paesi verso i quali i dati personali vengono trasmessi e su quale base giuridica ciò avviene (eventuali garanzie contrattuali o eccezioni utilizzate) [cfr. al riguardo il punto 3.9 e nell'allegato LISTA DI CONTROLLO 2: ATTUAZIONE DEI REQUISITI DELL'nLPD].

3.7 Estensione dei diritti delle persone interessate

Secondo l'nLPD, i diritti delle persone interessate a informazioni, cancellazione o blocco (limitazione) dei loro dati personali rimangono invariati e vengono parzialmente adeguati. Le persone interessate hanno diritto a tutte le informazioni necessarie per far valere i loro diritti e garantire un trattamento trasparente dei dati (art. 25 cpv. 2 nLPD). In linea di principio, l'informazione è gratuita e deve essere fornita entro 30 giorni (art. 25

cpv. 6 e 7 nLPD). Viene introdotto anche un diritto alla portabilità dei dati (art. 28 ss. nLPD). Di conseguenza, ogni persona può chiedere a un titolare del trattamento di fornirle i dati personali che la riguardano e che le sono stati comunicati in precedenza, nonché i dati personali trattati in modo automatizzato sulla base di un consenso o di un contratto, in un formato elettronico di uso corrente o di trasmettere tali dati a un altro titolare del trattamento (art. 28 nLPD).

3.8 Diritto di veto nel trattamento dei dati personali da parte dei responsabili del trattamento

Secondo la nuova legge sulla protezione dei dati, il trattamento dei dati personali può essere trasferito a terzi mediante accordo o per legge, se i dati sono trattati come dovrebbe fare il prestatore di personale stesso e non vi sono obblighi di riservatezza legali o contrattuali che vietino l'esternalizzazione (art. 9 cpv. 1 nLPD). Esempi di trasferimento del trattamento dei dati personali a terzi (appaltatori) sono i lavori di elaborazione dei dati per il conteggio dei salari, la contabilità finanziaria da parte dei centri di calcolo, l'esternalizzazione del trattamento dei dati a un fornitore di servizi IT basata sulla tecnologia cloud o l'impiego di fornitori di servizi per l'invio di newsletter. In questi casi, il titolare del trattamento rimane responsabile del trattamento dei dati. In questo modo deve garantire che il terzo incaricato garantisca la sicurezza dei dati (art. 8 cpv. 2 nLPD). D'ora in poi l'incaricato del trattamento può delegare il trattamento a terzi solo previa autorizzazione dell'impresa responsabile (cosiddetto diritto di veto) (art. 9 cpv. 3 nLPD). Eventuali violazioni della sicurezza dei dati devono essere segnalate al più presto dal responsabile del trattamento al titolare del trattamento (art. 24 cpv. 3 nLPD). Si raccomanda quindi di formulare un vincolo al rispetto degli obblighi di protezione dei dati in un allegato al rispettivo contratto con il fornitore di servizi o nelle CG. Un modello di questo tipo di formulazione nelle CG è riportato nell'allegato [ESEMPIO 3: MODELLO CLAUSOLA DI ELABORAZIONE DEGLI ORDINI NELLE CG].

3.9 Elenco dei Paesi con protezione dei dati equivalente pubblicato dal Consiglio federale

Ai sensi della nuova legge sulla protezione dei dati (nLPD), in caso di comunicazione di dati all'estero – come nel caso dell'impiego di un fornitore di servizi con sede all'estero (ad es. un fornitore di servizi IT con sede negli Stati Uniti) – occorre garantire che la personalità delle persone interessate non venga messa in pericolo. Il trasferimento di dati verso Paesi con una protezione dei dati equivalente e quindi l'esternalizzazione a società di outsourcing estere è senz'altro consentito (art. 16 cpv. 1 nLPD). I Paesi che prevedono una protezione dei dati equivalente sono pubblicati in un elenco. Sono inclusi la Svizzera e tutti i Paesi dell'UE. Da ora l'elenco dei Paesi con una protezione dei dati equivalente sarà pubblicato dal Consiglio federale e non più dal l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).

In mancanza di una legislazione che garantisca una protezione adeguata, i dati personali possono essere comunicati all'estero solo in presenza di garanzie sufficienti (art. 16 cpv. 2 nLPD). Tali garanzie sufficienti sono in particolare le clausole contrattuali tipo (SCC) della Commissione europea. Sono possibili eccezioni, ad esempio, se la persona interessata ha espressamente acconsentito alla comunicazione (art. 17 cpv. 1 lett. a nLPD).

3.10 Obbligo di notifica in caso di violazione della sicurezza dei dati

In caso di violazione dei dati, l'impresa responsabile deve notificare il più rapidamente possibile all'IFPDT (ed eventualmente alle persone interessate) le violazioni della sicurezza dei dati che possono rappresentare un rischio elevato per le persone interessate (art. 24 cpv. 1 nLPD). Ciò include, ad esempio, il furto di dati personali da parte di persone interne o esterne (ad esempio hacker) o la distruzione di informazioni, ad

esempio a causa di errori dell'utente, errori tecnici, virus o attacchi da parte di hacker. Di norma, la segnalazione dovrebbe essere autorizzata dalla direzione. In ultima analisi, tuttavia, sono i membri del consiglio di amministrazione i responsabili della gestione dei rischi (cfr. art. 754 cpv. 1 CO). L'azienda responsabile deve documentare le violazioni. La documentazione deve contenere i fatti relativi agli eventi, le loro conseguenze e i provvedimenti adottati. Deve essere conservata per almeno due anni dalla data della segnalazione (art. 15 cpv. 4 OPDa).

3.11 Nuovi obblighi formali secondo nLPD

In futuro i prestatori di personale dovranno rispettare gli obblighi formali in relazione al trattamento dei dati personali:

- designazione di un ufficio centrale per la protezione dei dati (ad es. servizio giuridico, IT).
- Un'impresa con più di 250 collaboratori deve tenere un registro delle attività di trattamento dei dati personali (art. 12 nLPD). Tra i 250 collaboratori devono essere conteggiati anche collaboratori temporanei. In casi eccezionali, anche le imprese con meno di 250 collaboratori devono tenere un registro, vale a dire se trattano dati personali degni di particolare protezione su vasta scala o se effettuano attività di profilazione ad alto rischio.
- L'elenco del titolare del trattamento deve contenere almeno le seguenti informazioni:
  - identità del responsabile;
  - finalità del trattamento;
  - descrizione delle categorie di persone interessate e delle categorie di dati personali trattati;
  - categorie dei destinatari;
  - la durata di conservazione dei dati personali o i criteri per determinare tale durata;
  - descrizione delle misure di sicurezza dei dati e
  - in caso di comunicazione all'estero, indicazione dello Stato e garanzia che assicura un'adeguata protezione dei dati.
- Il prestatore di personale, in qualità di responsabile ai sensi dell'nLPD, deve mettere in atto misure tecniche e organizzative per la sicurezza delle informazioni al fine di proteggere adeguatamente i dati personali (art. 8 nLPD) (cfr. in allegato il link alla Guida ai provvedimenti tecnici e organizzativi concernenti la protezione dei dati con riferimento all'attuale LPD dell'IFPDT: LINK UTILI).
- L'azienda responsabile deve prima elaborare una valutazione d'impatto sulla protezione dei dati (DPIA) se un trattamento può comportare un rischio elevato per la personalità o i diritti fondamentali delle persone interessate. Per progetti più delicati, come l'introduzione di applicazioni speciali, è quindi obbligatorio eseguire e documentare un'analisi formalizzata dei rischi. Quando sussiste un rischio elevato, deriva da diverse circostanze, in particolare dall'impiego di nuove tecnologie, dal tipo, dalla portata, dalle circostanze e dallo scopo del trattamento dei dati personali. La DPIA stessa contiene una descrizione del trattamento previsto, una valutazione dei rischi per la personalità o i diritti fondamentali della persona interessata e le misure adottate in questo contesto per proteggere la personalità e i diritti fondamentali. Si tratta quindi essenzialmente di un'analisi dei rischi (art. 22 s. nLPD). Alcuni Cantoni, come ad esempio il Canton Zurigo, hanno pubblicato moduli per l'elaborazione di una DPIA [cfr. allegato: LINK UTILI].
- In conclusione, anche i collaboratori devono essere sensibilizzati e formati in materia di protezione dei dati.

4. Sanzioni

Con l'nLPD, anche le sanzioni sono aumentate in modo significativo. Chiunque violi intenzionalmente gli obblighi dell'nLPD (compresa l'eventuale adozione intenzionale del comportamento sanzionato) deve aspettarsi una multa fino a 250'000 franchi (art. 66 ss. nLPD) in caso di:

- informazioni false e incomplete;
- violazione degli obblighi di informazione;
- mancato rispetto dei requisiti minimi di sicurezza dei dati;
- trasferimento illecito all'estero;
- elaborazione degli ordini non conforme alle disposizioni di legge;
- violazione dell'obbligo di riservatezza.

Ciò significa che, secondo l'nLPD, i responsabili aziendali come CEO, CFO o CIO possono essere sanzionati direttamente. Dopo tutto, la maggior parte delle disposizioni penali sono reati punibili a querela di parte, quindi la violazione viene perseguita solo se una persona interessata presenta una denuncia penale.

5. Necessità d'intervento per i prestatori di personale svizzeri

N. 1 **Verifica sito web** (Informativa sulla protezione dei dati, CG, applicazioni, invio di newsletter, dichiarazioni di consenso)	**N. 2** **Verifica / stipula di contratti in caso di trattamento dei dati da parte di terzi (incl. trasferimento dei dati all'estero)** (contratto, diritto di impartire istruzioni, nessuna violazione degli obblighi di riservatezza, sicurezza dei dati, diritto di veto, obbligo di segnalazione in caso di trasmissione dei dati, eventualmente garanzie adeguate)
N. 3 **Verificare il rispetto dei principi di protezione dei dati** (liceità, buona fede, proporzionalità, finalità, correttezza dei dati, sicurezza dei dati)	**N. 4** **Elaborazione del processo di notifica in caso di violazione della sicurezza dei dati** (in caso di rischio elevato per l'IFPDT/persona interessata)
N. 5 **Elaborazione di processi relativi ai diritti degli interessati** (processo di informazione, processo di rettifica, processo di cancellazione, processo di opposizione, processo di portabilità dei dati)	**N. 6** **Rispetto degli obblighi formali** (ufficio centrale per la protezione dei dati, formazione del personale, elenco delle attività di trattamento a partire da 250 collaboratori DPIA)

Per la necessità concreta di intervento per i prestatori di personale si veda anche l'allegato LISTA DI CONTROLLO 2: ATTUAZIONE DEI REQUISITI DELL'nLPD.

Per eventuali domande, il servizio giuridico di swissstaffing è a disposizione al numero 044 / 388 95 75 o all'indirizzo legal@swissstaffing.ch.

Zurigo, marzo 2023

swissstaffing

LISTA DI CONTROLLO 1: ADEGUAMENTI DAL GDPR UE ALL'nLPD

Se avete già implementato i requisiti del GDPR UE, questa lista di controllo vi consente di verificare quali adeguamenti devono ancora essere implementati in vista della revisione della legge sulla protezione dei dati.

Importante: È possibile che oltre all'nLPD si applichi anche il GDPR UE, motivo per cui è possibile che i requisiti si applichino in parallelo.

<table>
<tr><td>N. 1</td><td>Applicabilità dell'nLPD

Spesso nei documenti elaborati si fa riferimento solo al GDPR UE. Ora questo riferimento deve essere ampliato e deve essere inclusa anche l'nLPD.</td><td>Oltre all'applicazione del GDPR UE, si fa riferimento anche all'applicazione dell'nLPD.</td><td>☐</td></tr>
<tr><td>N. 2</td><td>Terminologia

I termini dell'nLPD sono leggermente diversi rispetto a quelli del GDPR UE:

<table><tr><th>nLPD</th><th>GDPR UE</th></tr><tr><td>trattamento</td><td>elaborazione</td></tr><tr><td>dati personali degni di particolare protezione</td><td>categorie particolari di dati personali</td></tr><tr><td>violazione della sicurezza dei dati</td><td>violazione della protezione dei dati</td></tr></table></td><td>Nei documenti sono stati adattati i seguenti termini: elaborazione/trattamento, categorie particolari di dati/dati degni di particolare protezione, violazione della protezione dei dati/violazione della sicurezza dei dati</td><td>☐</td></tr>
<tr><td>N. 3</td><td>Definizione estesa di dati degni di particolare protezione

I dati relativi a procedimenti amministrativi e penali o a sanzioni e i dati relativi a misure di assistenza sociale sono considerati dati personali degni di particolare protezione ai sensi della nuova legge sulla protezione dei dati (nLPD). Di conseguenza, se necessario, occorre richiedere un consenso esplicito in tal senso.</td><td>Ove necessario, il trattamento di dati relativi a procedimenti amministrativi e penali o a sanzioni e di dati relativi a misure di assistenza sociale richiede il consenso esplicito.</td><td>☐</td></tr>
<tr><td>N. 4</td><td>Adempimento degli obblighi di informazione

Gli obblighi di informazione in vigore per la Svizzera prevedono alcune differenziazioni rispetto al GDPR UE. La dichiarazione sulla protezione dei dati deve riportare l'indicazione del Paese di destinazione in</td><td>La dichiarazione sulla protezione dei dati è stata integrata con il Paese di destinazione in caso di trasferimento dei dati</td><td>☐</td></tr>
</table>

	caso di trasferimento di dati all'estero.	all'estero.	
N. 5	**Elenco delle attività di trattamento** Se i dati personali devono essere trasmessi all'estero, nell'elenco delle attività di trattamento secondo l'nLPD deve essere indicato il Paese di destinazione.	L'elenco delle attività di trattamento è stato completato con l'indicazione di un Paese di destinazione del trattamento dati.	☐
N. 6	**Processo violazione della sicurezza dei dati** Ai sensi del GDPR UE, le cosiddette violazioni dei dati con rischio per le persone interessate devono essere segnalate entro 72 ore (furto e abuso di dati). Ai sensi dell'nLPD, una violazione della sicurezza dei dati deve essere segnalata il più rapidamente possibile all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), laddove comporti un rischio elevato per le persone interessate. La soglia di rischio che fa scattare l'obbligo di notifica all'autorità di protezione dei dati e/o alle persone interessate è quindi definita in modo diverso nella nuova legge sulla protezione dei dati rispetto al GDPR UE.	Il termine dell'obbligo di notifica è stato modificato da 72 ore a «il più rapidamente possibile» e la soglia di rischio è stata adeguata.	☐
N. 7	**Processo richiesta persone interessate** A differenza del GDPR UE, l'nLPD contiene, oltre alle informazioni minime che devono essere fornite in ogni caso a una persona interessata che richiede informazioni, una regola generale secondo cui una persona interessata riceve le informazioni necessarie per far valere i propri diritti e garantire un trattamento trasparente dei dati.	La procedura per le richieste delle persone interessate è stata completata con la possibilità per una persona interessata di ricevere le informazioni necessarie per far valere i propri diritti e per garantire un trattamento trasparente dei dati.	☐
N. 8	**Obbligo di protocollazione** A differenza del GDPR UE, l'nLPD non prevede nessuna «responsabilità» generale. Nel contesto della sicurezza dei dati, tuttavia, per il trattamento di dati personali degni di particolare protezione su	Se i dati personali degni di particolare protezione vengono trattati in modo automatizzato su larga scala o se viene eseguita una profilazione a rischio	☐

	vasta scala e per l'esecuzione di una profilazione a rischio elevato si applicano obblighi più ampi rispetto al GDPR UE, laddove le misure preventive non garantiscano la protezione dei dati. Per la memorizzazione, la modifica, la lettura, la comunicazione, la cancellazione e la distruzione di dati si applica pertanto un obbligo di protocollazione e deve essere redatto un regolamento sul trattamento con indicazioni sull'organizzazione interna, sulla procedura di trattamento e di controllo dei dati nonché sulle misure volte a garantire la sicurezza dei dati (art. 4 OPDa). In particolare la protocollazione deve avvenire anche se diversamente non è possibile stabilire a posteriori se i dati sono stati trattati per gli scopi per i quali sono stati acquisiti o comunicati.	elevato e le misure preventive non garantiscono la protezione dei dati, vengono rispettate le prescrizioni relative alla protocollazione.	

swissstaffing

LISTA DI CONTROLLO 2: ATTUAZIONE DEI REQUISITI DELL'nLPD

Questa lista di controllo consente di implementare i requisiti dell'nLPD e di verificare il proprio status quo.

N. 1	**Verifica del sito web** Il sito web è il proprio biglietto da visita. È liberamente e pubblicamente accessibile. La dichiarazione sulla protezione dei dati informa sul trattamento dei dati personali e soddisfa quindi i requisiti dell'obbligo di informazione ai sensi dell'nLPD.	L'informativa sulla privacy è corretta, completa e aggiornata.	☐
		L'informativa sulla privacy è collocata in una posizione ben visibile sul sito web.	☐
		Se il sito web è disponibile in più lingue, la dichiarazione sulla protezione dei dati è stata tradotta nelle rispettive lingue.	☐
		Se sono presenti condizioni generali di contratto (CG), la conformità alla protezione dei dati è stata verificata.	☐
		Se viene inviata una newsletter, la conformità alla protezione dei dati è stata verificata.	☐
N. 2	**Verifica/stipula di contratti in caso di trattamento dei dati da parte di terzi (incl. trasferimento di dati all'estero)** Esempi: Contratti con fornitori di servizi IT relativi all'esternalizzazione del trattamento dati basata sulla tecnologia cloud o a contratti con fornitori di servizi per la creazione di buste paga dei dipendenti del prestatore di personale. In base all'nLPD, il trattamento dei dati personali può essere trasferito a terzi su accordo o per legge, se i dati sono trattati come prestatore di personale stesso dovrebbe fare e non vi sono obblighi di riservatezza legali o contrattuali che vietano l'esternalizzazione. Inoltre, l'impresa committente deve assicurare che il terzo incaricato garantisca la sicurezza dei dati (art. 9 cpv. 1 e 2 nLPD). Da ora il responsabile del trattamento può delegare l'elaborazione a un terzo solo	La conformità alla protezione dei dati dei contratti con i fornitori di servizi è stata controllata.	☐
		Sono state concordate clausole contrattuali tipo UE con un fornitore di servizi in un Paese senza un livello adeguato di protezione dei dati o altre garanzie adeguate e, laddove necessario, sono state adottate misure aggiuntive.	☐

	previa autorizzazione del titolare del trattamento (diritto di veto) (art. 9 cpv. 3 nLPD). Eventuali violazioni della sicurezza dei dati devono essere segnalate al più presto dal responsabile del trattamento al titolare del trattamento (art. 24 cpv. 3 nLPD). La responsabilità del trattamento dei dati rimane del prestatore di personale (fornitore di outsourcing). In caso di comunicazione di dati all'estero, occorre garantire che la personalità delle persone interessate non venga messa in pericolo.		
N. 3	**Verificare il rispetto dei principi di protezione dei dati** Si tratta della legalità, della destinazione vincolata, della buona fede, della proporzionalità e della correttezza dei dati, eventualmente del consenso, della sicurezza dei dati, della Privacy by Design e della Privacy by Default.	È stato verificato il rispetto dei principi nell'ambito del trattamento dei dati personali.	☐
		I requisiti per la sicurezza dei dati sono garantiti.	☐
		È stato verificato dove è necessario il consenso e, se del caso, ne è stata garantita la fornitura.	☐
		I principi Privacy by Design e Privacy by Default sono tenuti in debita considerazione.	☐
N. 4	**Elaborazione di una procedura di segnalazione in caso di violazione della sicurezza dei dati**	È stato elaborato un processo per reagire il più rapidamente possibile in caso di incidenti relativi alla sicurezza dei dati e per comunicare l'incidente all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) ed eventualmente informare le persone interessate.	☐
N. 5	**Elaborazione dei relativi processi in caso di richieste da parte di persone interessate**	Esiste una procedura da seguire in caso di richieste da parte di persone interessate, in modo che ricevano le informazioni necessarie per far valere i loro diritti e in modo da garantire un trattamento trasparente dei dati. Di norma le informazioni devono essere fornite entro 30	☐

		giorni.	
N. 6	**Rispetto degli obblighi formali**	È stato designato un punto di contatto centrale per tutte le questioni relative alla protezione dei dati (ad es. servizio giuridico, IT); se necessario, è stato nominato un consulente per la protezione dei dati ai sensi dell'articolo 10 dell'nLPD, quest'ultimo deve disporre delle conoscenze specialistiche necessarie. Inoltre, deve essere tecnicamente indipendente e non vincolato da istruzioni nei confronti del titolare del trattamento e non può svolgere attività incompatibili con i suoi compiti.	☐
		Se necessario, è stato redatto un elenco delle attività di trattamento.	☐
		Se necessario, è stata effettuata una valutazione d'impatto sulla protezione dei dati (DPIA).	☐
		I collaboratori sono stati formati in merito ai requisiti dell'nLPD e alle misure adottate in azienda.	☐
		Se i dati personali degni di particolare protezione vengono trattati in modo automatizzato su larga scala o se viene eseguita una profilazione ad alto rischio e le misure preventive non garantiscono la protezione dei dati, vengono rispettate le prescrizioni relative alla protocollazione.	☐

swissstaffing

ESEMPIO 1: MODELLO CLAUSOLA DI CONSENSO

[*Questo modello è incompleto ed esemplificativo e deve essere adattato al singolo caso*]

Trattiamo i documenti di candidatura in modo strettamente confidenziale e li utilizziamo solo per lo scopo concordato.

- Collocamento del personale: I dati vengono trattati solo nella misura e per il tempo necessari per il collocamento. I dati possono essere trasmessi a potenziali datori di lavoro.
- Prestito di personale: I dati vengono elaborati fino alla fine del rapporto di prestito e i profili possono essere trasmessi a potenziali aziende acquisitrici.

Senza il relativo consenso, il dossier di candidatura (elettronico) viene cancellato/distrutto dopo la conclusione della procedura di candidatura, a meno che non sia soggetto a un obbligo di conservazione previsto dalla legge.

Acconsento espressamente alla successiva elaborazione, memorizzazione o trasmissione dei miei dati personali:

☐ Acconsento a che i miei dati personali, che ho comunicato in concomitanza con la mia candidatura, possano essere memorizzati, trattati o trasmessi all'interno delle società di [prestatore di personale] in Svizzera e all'estero [se non viene fornita un'adeguata protezione dei dati: indicazione del Paese] ai fini del prestito e/o del collocamento del personale.

☐ Acconsento a che i miei dati personali, che ho comunicato in concomitanza con la mia candidatura, possano essere memorizzati, trattati e comunicati a terzi in Svizzera e all'estero durante la procedura di collocamento e oltre la fine della procedura concreta di collocamento ai fini del prestito e/o del collocamento del personale. Queste terze parti sono, tra l'altro, società collegate a [prestatore di personale], fornitori di servizi che mettono a disposizione e gestiscono applicazioni IT utilizzate, nonché altre società che partecipano alle operazioni necessarie per la fornitura dei servizi contrattuali di [prestatore di personale] (ad es. fornitori di servizi di pagamento). In quanto a questo, acconsento al trasferimento dei miei dati anche in Paesi [indicare il Paese] in cui non esiste un livello adeguato di protezione dei dati. Se in relazione alla mia candidatura ho comunicato dati personali degni di particolare protezione ai sensi dell'art. 5 lett. c nLPD (ad es. una foto che mostra l'origine etnica, ecc.), il mio consenso si riferisce anche a questi dati.

☐ Acconsento all'invio di newsletter da parte di [prestatore di personale] all'indirizzo e-mail da me fornito. Queste newsletter contengono in particolare informazioni sulle offerte di lavoro che potrebbero essere di mio interesse.

I consensi sono indipendenti l'uno dall'altro e sono volontari. Posso revocare il mio consenso in qualsiasi momento senza indicarne i motivi e ho il diritto di richiedere la cancellazione dei miei dati personali in qualsiasi momento. Posso annullare l'iscrizione tramite il link alla fine di ogni newsletter. Prendo atto che, in caso di revoca del mio consenso al trattamento dei miei dati personali (ad eccezione del consenso alla ricezione della newsletter via e-mail), i servizi offerti da [prestatore di personale] non potranno essere ulteriormente forniti e si arriverà alla cessazione dei rapporti contrattuali.

swissstaffing

ESEMPIO 2: MODELLO CLAUSOLE DI PROTEZIONE DEI DATI E DI CONSENSO NELLE CG

[*Questo modello è incompleto ed esemplificativo e deve essere adattato al singolo caso*]

Protezione dei dati

Le parti si impegnano a rispettare in ogni momento le direttive vigenti in materia di protezione dei dati. Nell'ambito del rispettivo contratto, [prestatore di personale] è autorizzato a raccogliere, elaborare e divulgare i dati dei collaboratori, degli amministratori delegati e di altri dipendenti del cliente (di seguito i «dati personali» del cliente) per tutti gli scopi relativi all'adempimento del contratto. Ciò include, in particolare, il trasferimento dei dati personali del cliente all'estero per gli scopi di cui sopra, che potrebbe essere necessario per l'adempimento del contratto [fatta salva un'adeguata protezione dei dati: indicazione del Paese]. Inoltre, [prestatore di personale] è espressamente autorizzato a trattare i dati personali del cliente in qualsiasi forma e a divulgarli a eventuali società del gruppo o a terzi all'estero.

A questo mezzo il cliente acconsente all'utilizzo dei propri dati personali per scopi di marketing. Il cliente dichiara espressamente che tale consenso è in possesso delle persone interessate. [Prestatore di personale] può richiederlo al cliente in qualsiasi momento.

swissstaffing

ESEMPIO 3: MODELLO CLAUSOLA DI ELABORAZIONE DEGLI ORDINI NELLE CG

[*Questo modello è incompleto, esemplificativo e da adattare al singolo caso*]

Trattamento dei dati personali da parte di terzi (elaborazione degli ordini)

L'incaricato si impegna a trattare i dati personali trasmessigli o a lui accessibili nel settore di [prestatore di personale] solo nella misura ed esclusivamente per gli scopi necessari per l'adempimento del contratto.

L'incaricato si impegna ad adottare misure tecniche e organizzative adeguate per garantire la protezione dei dati e la sicurezza delle informazioni.

L'incaricato elabora i dati personali (incl. accessi e server web della sede) solo in Svizzera, nell'UE o nello Spazio economico europeo.

Già prima della conclusione del contratto, l'incaricato rende noti almeno i subappaltatori che trattano dati personali per suo conto. Esso vincola tutti i subincaricati, gli agenti e i terzi coinvolti agli obblighi derivanti dal presente contratto di elaborazione degli ordini. Per il coinvolgimento di ogni subappaltatore aggiuntivo, l'incaricato ottiene preventivamente il consenso scritto di [prestatore di personale]. In assenza di consenso scritto, l'incaricato non può nominare un altro subappaltatore. È a sola discrezione del committente accettare o rifiutare un terzo come futuro subappaltatore.

L'incaricato tratta in modo confidenziale tutti i dati personali acquisiti direttamente o indirettamente in relazione al contratto. In particolare, garantisce a [prestatore di personale] di non trasmettere i dati personali a terzi non autorizzati né di renderli accessibili in altro modo a terzi non autorizzati. L'obbligo di rispettare la riservatezza viene trasferito dall'incaricato a tutti i subappaltatori, agenti e terzi coinvolti.

L'incaricato assisterà [prestatore di personale] nel rispetto dei requisiti delle disposizioni applicabili in materia di protezione dei dati. In particolare, risponde tempestivamente e correttamente a tutte le richieste dell'incaricato in relazione al trattamento dei dati personali. Trasmette immediatamente le richieste delle persone o delle autorità interessate a [prestatore di personale] senza rispondere personalmente. L'incaricato è tenuto a collaborare a eventuali procedure prudenziali relative alle prestazioni che deve fornire e a mettere a disposizione le informazioni e i documenti da lui richiesti.

L'incaricato informa immediatamente [prestatore di personale] se è a conoscenza o sospetta che i dati personali da lui trattati per [prestatore di personale] siano stati esposti ad accesso non autorizzato, siano stati trasmessi a terzi non autorizzati, siano andati persi o danneggiati o siano stati o possano essere trattati in altro modo in violazione del diritto o del contratto. L'incaricato deve inoltre adottare subito le misure immediate necessarie per proteggere i dati personali e prevenire o ridurre al minimo eventuali conseguenze negative.

[Prestatore di personale] ha il diritto di controllare in qualsiasi momento il rispetto delle disposizioni applicabili in materia di protezione dei dati da parte dell'incaricato.

In caso di risoluzione del contratto, l'incaricato deve trasferire o distruggere i dati personali (comprese eventuali copie) che ha elaborato per [prestatore di personale], salvo diversa disposizione nel contratto, secondo le istruzioni esplicite di [prestatore di personale]. La distruzione dei dati deve essere documentata dall'incaricato e una copia di tale documentazione deve essere inviata spontaneamente a [prestatore di personale].

ALLEGATO: LINK UTILI

Messaggio concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati del 15 settembre 2017, il documento è disponibile qui

Comunicati stampa dell'Ufficio federale di giustizia sono disponibili qui e qui

Il sito web generale dell'Incaricato della protezione dei dati e della trasparenza (IFPDT) è disponibile qui

La guida alle misure tecniche e organizzative (2015) dell'IFPDT è disponibile qui

Il modulo per l'elaborazione di una valutazione d'impatto sulla protezione dei dati del Canton Zurigo è disponibile qui