LA NUOVA LEGGE FEDERALE SULLA PROTEZIONE DEI DATI (nLPD) A CONFRONTO CON IL REGOLAMENTO (UE) 2016/679 (GDPR)

(versione ITA/ENG)

07 Luglio 2022

fidinam & Partners
Consulenza fiscale, legale e societaria

LA NUOVA LEGGE FEDERALE SULLA PROTEZIONE DEI DATI (nLPD) A CONFRONTO CON IL REGOLAMENTO (UE) 2016/679 (GDPR)

Sono mesi ormai che si sente parlare di **nuova LPD**, di revisione totale della LPD; **ma che cos'è la LPD e perché una revisione totale**?
LPD è l'acronimo ufficiale della Legge (federale) sulla Protezione dei Dati. Il testo finale della **nuova LPD** (nLPD) è stato adottato il 25 settembre 2020, la sua entrata in vigore è prevista per il primo settembre 2023, anche se mancano tutt'ora le norme attuative.
L'obiettivo della LPD è di proteggere la personalità ed i diritti fondamentali delle persone i cui dati sono oggetto di trattamento (art. 1 della LPD).

Perché una revisione totale:

La prima legge federale sulla protezione dei dati del 19 giugno 1992 è entrata in vigore (1° luglio 1993) quando Internet non era ancora usato a scopi commerciali e non era possibile prevedere una realtà digitale caratterizzata da un'iper-connettività alla rete, il tutto accelerato dalle nuove tecnologie dell'informazione e dei mezzi di comunicazione (diffusione dei telefoni cellulari, dei social media) spesso estremamente connessi.

Inoltre il progresso tecnologico spinge il mondo giuridico ad una continua e attenta revisione. La tematica Protection & Privacy ha avuto il suo apice con il Regolamento (UE) 2016/679 (GDPR) direttamente applicabile per tutti gli stati UE dal 25 maggio 2018, con un impatto considerevole anche sulle aziende stabilite al di fuori dello Spazio Economico Europeo (SEE) ed in particolare in tema di trasferimento di dati personali verso paesi terzi (non SEE). Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è lecito se il titolare (Data Controller) o il responsabile del trattamento (Data Processor) possono fare valere certe garanzie (Art. 45 a 49 GDPR), tra cui la decisione di adeguatezza (art. 45 GDPR). La decisione di adeguatezza è un atto di esecuzione rilasciato dalla Commissione Europea a paesi terzi, riconosciuto "safe", ossia che garantisce un livello di protezione adeguato. In tale caso il trasferimento di dati personali non necessita di autorizzazioni specifiche previste dagli Art. 46 a 49 GDPR.

La revisione totale della LPD è volta, con la ratifica della Convenzione STE 108+ del Consiglio d'Europa sulla protezione e il suo adeguamento ai requisiti del regolamento (UE) 2016/679, ad assicurare alla Svizzera il rinnovo della decisione di adeguatezza da parte della Commissione Europea e permettere le comunicazioni transfrontaliere di dati senza ulteriori ostacoli.

Quali sono le principali novità della nLPD

Cosi come il GDPR, la nLPD si prefigge **di tutelare i dati personali delle persone fisiche** attraverso una maggiore trasparenza nei confronti delle persone interessate e la responsabilizzazione (principio di accountability) delle aziende (Data Controller o Data Processor del trattamento) con conseguenti obblighi di legge nei loro confronti e risvolti sanzionatori in caso di violazione o di inadempienze.
L'elemento fondamentale della revisione è il cosiddetto approccio basato sul rischio. La nLPD stabilisce degli obblighi ai quali le aziende devono conformarsi e che le consentano di rilevare per tempo i rischi per la personalità e i diritti

THE NEW FEDERAL ACT ON DATA PROTECTION (nFADP) COMPARED TO EU REGULATION 2016/679 (GDPR)

For months now, we have been hearing about a **new FADP**, a total revision of the FADP; **but what is the FADP and why a total revision?**
FADP is the official acronym for the Federal Act on Data Protection. The final text of the **new FADP** (nFADP) was adopted on 25 September 2020, and is scheduled to enter into force on 1 September 2023, although implementing regulations are still lacking.
The aim of the FADP is to protect the personality and fundamental rights of persons whose data has been processed (Art. 1 of the FADP).

Why a total overhaul?

The first Federal Data Protection Act of 19 June 1992 came into force (1 July 1993) when the Internet was not yet used for commercial purposes and a digital reality 2haracterized by hyper-connectivity to the network, all accelerated by new information and media technologies (spread of mobile phones, social media) that were often extremely connected, was unforeseen.

Furthermore, technological progress pushes the legal world to a continuous and careful revision. The topic of Protection & Privacy peaked with EU Regulation 2016/679 (GDPR), directly applicable for all EU states as of 25 May 2018, with a considerable impact also on companies established outside the European Economic Area (EEA) and in particular on the topic of transferring personal data to third (non-EEA) countries. The transfer of personal data to a third country or international organisation is lawful if the data controller (Data Controller) or data processor (Data Processor) can invoke certain safeguards (Arts. 45 to 49 GDPR), including the adequacy decision (Art. 45 GDPR). The adequacy decision is an implementing act issued by the European Commission to third countries that is recognised as 'safe', i.e. that guarantees an adequate level of protection. In such a case, the transfer of personal data does not require specific authorisations under Arts. 46 to 49 GDPR.

With the ratification of the Council of Europe's STE 108+ Convention on Data Protection and its adaptation to the requirements of EU Regulation 2016/679, the total revision of the FADP is intended to ensure that Switzerland will have its adequacy decision renewed by the European Commission and allow cross-border data communications without further obstacles.

What are the main innovations of the nFADP?

Like the GDPR, the nFADP aims **to protect the personal data of individuals** through greater transparency vis-à-vis the persons concerned and the empowerment (accountability principle) of companies (data controllers or data processors) with consequent legal obligations towards them and sanctions in the event of violations or non-compliance.
The core element of the review is the so-called risk-based approach. The nFADP establishes obligations with which companies must comply and which enable them to detect risks to the personality and fundamental rights of individuals

fondamentali delle persone al fine di eleminarli o eventualmente di mitigarli.

Gli obblighi di legge :

- Obbligo di protezione dei dati fino dalla progettazione (privacy by design) e per impostazione predefinita **Art. 7 nLPD**;
- Standard minimi di sicurezza **Art. 8 nLPD**;
- Registro dei trattamenti **Art. 12 nLPD**;
- Obbligo di informazione generalizzato a tutti i trattamenti di dati **Art. 19 nLPD**;
- Obbligo di valutazione d'impatto (DPIA) per i trattamenti che presentino un rischio elevato **Art. 22 nLPD** ;
- Obbligo di notifica e comunicazione in caso di Data Breach **Art. 24 nLPD**.

Specificità della nLPD rispetto al GDPR

I. **Principio di liceità**: il motivo giustificativo in Svizzera viene richiesto in presenza di un trattamento illecito, ossia un trattamento che rappresenta una violazione della personalità. L'**Art. 30 cpv 2 nLPD** fornisce esempi di illiceità del trattamento dei dati che possono comunque essere trattati in presenza di un motivo giustificativo (legge, consenso o interesse preponderante pubblico o privato).

II. l'Incaricato federale (IFPD) **non potrà pronunciare sanzioni amministrative** (pecuniarie), potrà prendere delle misure tra cui la modifica o la sospensione del trattamento dei dati o addirittura la cancellazione dei dati.

III. **Non è obbligatoria la figura del Data Protection Officer (DPO) nel settore privato**. La nomina di un DPO comporta (a determinate condizioni) l'esclusione dell'obbligo di consultazione preventiva dell'IFPD in presenza di trattamenti a rischio elevato dopo **una valutazione sulla protezione dei dati (DPIA**)

IV. **L'obbligo di informare l'interessato decade se il trattamento è obbligatorio per legge:** "nul n'est censé ignorer la loi".

V. In caso di **violazioni intenzionali** di determinati **obblighi** quali :

➔ obbligo di informare, di concedere l'accesso e di collaborare;
➔ obbligo di diligenza;
➔ obbligo del segreto;
➔ inosservanza di una decisione.

Sono previste delle **sanzioni penali** (**multe**) **a carico degli amministratori e/o dei managers fino ad CHF 250.000,-**. In caso di violazioni commesse nelle aziende (Art. 64 nLPD), se la multa non supera i CHF 50.000,- e se la determinazione degli autori della violazione richiede provvedimenti d'inchiesta sproporzionati, sarà l'azienda ad essere punita. Questa è una differenza sostanziale rispetto al GDPR, il quale istituisce pesanti sanzioni amministrative pecuniarie a carico delle aziende mentre la LPD

at an early stage in order to eliminate or possibly mitigate them.

Legal obligations:

- Duty of data protection by design and by default **Art. 7 nFADP;**
- Minimum Security Standards **Art. 8 nFADP;**
- Processing Register **Art. 12 nFADP;**
- Generalised duty to provide information on all data processing **Art. 19 nFADP;**
- Duty of impact assessment (DPIA) for high-risk processing **Art. 22 nFADP**;
- Duty of notification and disclosure in the event of a data breach **Art. 24 nFADP.**

Specificities of the nFADP versus the GDPR

I. **Principle of lawfulness**: the justifying reason is required in Switzerland in the presence of unlawful processing, i.e. processing that constitutes a violation of privacy. **Art. 30 para. 2 nFADP** gives examples of unlawful data processing that may nevertheless be processed if there is a justifying reason (law, consent or overriding public or private interest).

II. the Federal Data Protection Commissioner (FDPC) may **not pronounce administrative** (pecuniary) sanctions, he may take measures including modification or suspension of data processing or even deletion of data.

III. **The appointment of a Data Protection Officer (DPO) is not mandatory in the private sector.** The appointment of a DPO entails (under certain conditions) the exclusion of the obligation to consult the FDPC in advance in the case of high-risk processing operations **following a Data Protection Impact Assessment (DPIA)**

IV. **The obligation to inform the data subject lapses if the processing is obligatory by law**: 'nul n'est censé ignorer la loi – No one is supposed to ignore the law'.

V. In the case of **willful violations** of certain **obligations** such as:

➔ obligation to inform, to grant access and to cooperate;
➔ duty of care;
➔ obligation of secrecy;
➔ failure to comply with a decision.

Criminal **sanctions (fines) of up to CHF 250,000.- are in place for directors and/or managers.** In the case of violations committed in companies (Art. 64 nFADP), if the fine does not exceed CHF 50,000.- and if determining the perpetrators requires disproportionate investigative measures, it is the company that will be punished. This is a substantial difference from the GDPR, which imposes heavy administrative fines on companies, whereas the FADP has opted for making managers and decision-makers, accountable.

ha optato per la responsabilizzazione dei dirigenti, detentori del potere decisionale.

VI. Esistono **standard minimi di sicurezza:** approccio classico basato sui rischi quale elemento fondamentale della revisione della legge sulla protezione dei dati **(Art. 8** nLPD). Il Data Controller e il Data Processor del trattamento devono determinare i provvedimenti adeguati in base al rischio che di volta in volta si presenta. Compete al Consiglio Federale di emanare i **requisiti minimi di sicurezza** (**Art.8 cpv 3 nLPD**). **Gli Art. 1 a 3 dell'Ordinanza relativa alla LPD (P-OLPD)** non prescrivono requisiti minimi rigidi validi per tutti, ma intendono illustrare criteri di base di valutazione (i principi) e forniscono direttive volte a definire dei provvedimenti stilando un elenco di obiettivi di protezione (**art. 1 e 2 P-OLPD**). È inoltre stato consolidato e concretizzato l'obbligo di verbalizzazione (**art. 3 P-OLPD**). Quindi il Data controller e il Data Processor del trattamento dovranno verbalizzare tutti i trattamenti per i quali sussiste un rischio elevato per la personalità o i diritti fondamentali delle persone interessate.

VI. There are **minimum security standards**: classic risk-based approach as a fundamental element of the revision of the Data Protection Act (Art. 8 nFADP) . The Data Controller and the Data Processor of the processing operation must determine the appropriate measures on the basis of the risk arising from time to time. The Federal Council is responsible for **issuing the minimum security requirements (Art. 8 para. 3 nFADP). Arts. 1 to 3 of the Ordinance on the FADP (P-OFADP)** do not stipulate rigid minimum requirements that apply to everyone, but are intended to illustrate basic assessment criteria (the principles) and provide guidelines for measures by drawing up a list of protection objectives (**Arts. 1 and 2 P-OFADP**). In addition, the obligation to report has been strengthened and formalised (**Art. 3 P-POFADP**). Thus, the data controller and the data processor must keep minutes of all processing operations for which there is a high risk for the personality or fundamental rights of the data subjects.

Anche se l'approccio della nLPD è assimilabile al GDPR, la normativa svizzera intende mantenere la sua specificità come ad esempio in caso di notifica di Data Breach presso l'autorità garante, il GDPR prevede una notifica entro 72 ore (Art. 33 GDPR) mentre la nLPD richiede una notifica quanto prima (Art. 24 nLPD).

Although the approach of the nFADP is similar to the GDPR, the Swiss regulation intends to maintain its specificity, e.g. in the case of a data breach notification to the supervisory authority, the GDPR requires notification within 72 hours (Art. 33 GDPR) whereas the nFADP requires notification as soon as possible (Art. 24 nFADP).

Conclusioni

La nLPD e il GDPR sono due normative equiparabili ma che per molti aspetti presentano delle differenze sostanziali.
Occorre anche evidenziare che in relazione al campo di applicazione territoriale delle due normative e in riferimento al cosiddetto principio degli effetti, la nLPD si applica anche alle aziende estere che operano nel mercato svizzero o il cui trattamento dei dati ha effetti in Svizzera così come il GDPR si applica ad aziende svizzere che offrono beni o prestazioni di servizi nell'UE e esercitano un monitoraggio del comportamento dell'utente all'interno del territorio UE (Art. 3.2 GDPR).
Sicuramente una delle difficoltà per le aziende nel processo di messa in conformità alla nLPD, sarà l'identificazione del quadro normativo per la tutela della privacy e la protezione dei dati ed in particolare verificare se essa rientra nel campo di applicazione del GDPR o di qualsiasi altra normative estere.

Considerando la **complessità degli adempimenti e l'assenza di un termine generale di adeguamento** dopo l'entrata in vigore della nLPD, è auspicabile che il processo di messa in conformità venga avviato il prima possibile **con il supporto adeguato.** In questo modo, l'azienda oltre a dimostrare la **sua compliance alla norma**, potrà dimostrare che **tratta i dati personali dei suoi clienti, utenti, dipendenti nel rispetto dei loro diritti fondamentali della personalità**.

Conclusions

The nFADP and the GDPR are two regulations that are comparable but in many respects differ substantially.
It should also be pointed out that with regard to the territorial scope of application of the two regulations and with reference to the so-called principle of effects, the nFADP also applies to foreign companies that operate in the Swiss market or whose data processing has effects in Switzerland in the same way that the GDPR applies to Swiss companies that offer goods or services in the EU and monitor user behaviour within the EU (Art. 3.2 GDPR).
Undoubtedly one of the difficulties for companies in the nFADP compliance process will be identifying the legal framework for privacy and data protection and in particular whether it falls under the GDPR or any other foreign legislation.

Considering **the complexity of the requirements and the absence of a general deadline for compliance** after the entry into force of the nFADP, it is desirable to start the compliance process as soon as possible **with the appropriate support**. In this way, the company will not only be able to prove **its compliance with the standard**, but also to demonstrate **that it treats the personal data of its customers, users, and employees with respect for their fundamental personal rights.**

Isabel Costa
Manager Privacy
Fidinam & Partners SA
isabel.costa@fidinam.ch
T: +41 91 9731362

Fidinam & Partners SA
Via Maggio 1
6900 Lugano
www. fidinam-and-partners.ch