July 2023

changes to Swiss data protection law for employers

Top 10

On 1 September 2023, new data protection rules will enter into force in Switzerland.

These changes will have a number of effects with regard to employer obligations vis-à-vis employee personal data. To help you prepare for these changes and make any adaptations needed before the new rules enter into force, kindly find below an overview of the top 10 changes to be introduced by the new Federal Act on Data Protection ("**nFADP**") likely to affect employers, as well as the consequences of these changes for employers.

walderwyss attorneys at law

By Rayan Houdrouge
lic. iur., LL.M., Attorney at Law,
Certified Specialist SBA Labour Law,
Certified Social Security Expert
Partner
Phone +41 58 658 30 90
rayan.houdrouge@walderwyss.com

and Kathryn Kruglak
MLaw, LL.M., Attorney at Law
Associate
Phone +41 58 658 30 91
kathryn.kruglak@walderwyss.com

1. Scope

(i) Geographic scope: the nFADP applies to any action that has effects in Switzerland, even those that occur abroad. There fore, the nFADP also may apply to non-Swiss employers who have employees in Switzerland or who second employees to or from Switzerland.

(ii) Personal scope: the nFADP only applies to individuals' personal data. It does not apply to the personal data of companies and other legal persons. Therefore, companies do not themselves benefit from the data protection afforded to their employees.

(iii) Material scope: under the nFADP, genetic and biometric data also are considered sensitive data, meaning their collection and processing are subject to additional protective measures (e.g. express consent required for their collection). Therefore, employers who incorporate biometric data into their security system would need to take additional measures with regard to the collection and processing of this data.

2. Data Protection Officer

The nFADP extends the position of Swiss Data Protection Officer ("**CH DPO**"), also sometimes referred to as the Data Protection Advisor.

The CH DPO: (*i*) trains and advises the data controller on data protection, and (*ii*) assist with the application of data protection rules.

Under the nFADP there still is no requirement to appoint a CH DPO, although voluntarily doing so may dispense the data controller of certain obligations (i.e. notification of the impact assessment – see *Point 3* below), provided:

(i) the CH DPO performs their duties independently of, and without receiving instructions from, the data controller;

(ii) the CH DPO does not carry out tasks incompatible with their duties as CH DPO;

(iii) the CH DPO has the necessary professional knowledge; and

(iv) the contact information for the CH DPO is published by the data controller and communicated to the Federal Data Protection and Information Commissioner ("**FDPIC**").

Therefore, employers may appoint a CH DPO to assist with data protection. Moreover, this individual may be part of the company or an external data protection officer.

3. Impact assessment

The nFADP requires the data controller to carry out a data protection impact assessment when the data processing could pose a high risk to the data subject (e.g. risk of illicit collection or processing, risk of sensitive data being transferred to a third party, risk of a security breach, risk of "data matching" that makes it possible to assess fundamental characteristics of an individual, such as consumer habits, etc.).

Pursuant to the nFADP, a high risk automatically exists when there is mass processing of sensitive personal data or systematic surveillance of large parts of the public domain. Further, in particular, there also may be a high risk when new technology is used.

Therefore, employers in this situation (e.g. using new technology to process employee personal data) must carry out a data protection impact assessment, which must: (*i*) include a description of the data processing that is planned; (*ii*) evaluate the risks; and (*iii*) enumerate the

measures that will be taken to mitigate the risks.

Exceptions to this requirement exist, in particular, when: (*i*) the data controller is legally required to carry out the data processing; (*ii*) the data controller is using a system, process or service certified pursuant to the nFADP; or (*iii*) the data controller is processing data in accordance with a code of conduct (e.g. codes established by professional associations) meeting the conditions posed by the nFADP and approved by the FDPIC.

Moreover, unless a CH DPO has been appointed (see *Point 2* above for the conditions), the data controller must consult with the FDPIC prior to processing any data if the impact assessment shows that, despite the proposed mitigation measures, the planned processing still could pose a high risk to the data subject.

4. Privacy notice

Under the nFADP, the data subject must be provided with a privacy notice with information about the collection and processing of personal data whenever personal data are collected.

Therefore, employers must provide employees with a privacy notice containing at least the following information:

(i) the identity and contact details of the data controller;

(ii) the purpose of the processing; and

(iii) if applicable, the recipients or categories of recipients to whom personal data will be disclosed.

If data are transferred abroad, the privacy notice also must contain (*iv*) the name of the State(s) or international body(ies) to which the data are communicated and, if the State to which the data are disclosed does not have adequate protections, (*v*) the safeguards or derogations relied upon.

The privacy notice may be provided directly to employees or made available online (e.g. employee intranet), provided it is easily accessible.

5. Record of processing activities

Under the nFADP, it is obligatory to keep a record of processing activities ("ROPA").

Therefore, employers must keep a ROPA containing at least the following information:

(i) the identity of the data controller;

(ii) the purpose of the processing;

(iii) a description of the categories of data subjects whose personal data were processed and the categories of personal data processed;

(iv) the recipients to whom personal data will be disclosed;

(v) how long the personal data will be stored or the criteria used to determine the length of storage;

(vi) a general description of the measures taken to guarantee data security; and

(vii) if applicable (i.e. data are transferred abroad), the name of the State(s) and, if necessary, the safeguards relied upon.

When the employer makes use of subcontractors, the subcontractors also must keep a ROPA.

That said, there are exceptions to this obligation. Provided there is no mass processing of sensitive personal data or high-risk profiling (i.e. profiling that presents a high risk to the data subject, because it leads to "data matching"), companies with fewer than 250 employees on 1 January of a given year do not need to keep a ROPA. This same exception applies to individual employers.

6. Outsourcing data processing

The data controller may outsource data processing to a subcontractor, provided certain conditions are met.

For instance, an employer may outsource the processing of employee personal data to a subcontractor providing payroll services, provided: (*i*) the subcontractor only carries out data processing that the data controller is entitled to carry out, and (*ii*) the outsourcing is not prohibited by a legal or contractual duty to maintain secrecy.

The data controller also must ensure that the subcontractor can guarantee the security of the data.

Moreover, the subcontractor may not further outsource data processing to another subcontractor without the prior approval of the data controller.

7. Automated decisions (profiling)

Under the nFADP, the data subject must be informed when an automated decision is made (i.e. a decision made exclusively based on the automated processing of personal data) when this decision has legal effects for the data subject or significantly affects the data subject.

The data subject also must be informed of the possibility to submit their opinion regarding this decision and request that it be reviewed by a human.

Therefore, employers may not rely entirely on automated measures (e.g. algorithms) to terminate employees or take disciplinary measures against employees.

8. Security breaches

Data controllers must notify the FDPIC promptly in the event of a data security breach that likely poses a high risk to the data subject's personal or fundamental rights (e.g. medical data or other sensitive data, data that could be used to usurp the data subject's identity, etc.).

Subcontractors must notify the FDPIC promptly in the event of any data security breach.

Moreover, the data subject must be notified of the data security breach when it is necessary for their protection (e.g. they may need to take certain steps, such as monitoring their credit report, data may have been obtained by a party who wishes to harm them, etc.) or required by the FDPIC.

Therefore, given the type of employee personal data that an employer tends to have on file, in the event of a data security breach, the employer likely would need to inform the FDPIC of the breach and, in some instances, also may need to inform employees.

9. Powers of the FDPIC

The nFADP gives additional oversight, investigative and decision-making powers to the FDPIC.

In particular, the FDPIC can order the modification, suspension or cessation of all or some of the personal data processing, as well as the deletion or destruction of all or some of the personal data. Also, under certain circumstances, the FDPIC can suspend or prohibit the transfer of data abroad and require that certain documents and information be handed over.

Moreover, the FDPIC can issue administrative fines in the event of non compliance with its decisions.

Therefore, the FDPIC could stop an employer (*i*) from collecting and processing certain personal data, in particular, personal data that do not concern employees' suitability for their job and are not necessary for the performance of the employment contract, or (*ii*) from transferring data abroad (e.g. to a group company in a State without adequate protections, without having taken appropriate measures).

10. Criminal fines

Violations of the nFADP, including violations with regard to the privacy notice, information about automated decisions and the duty of discretion, can result in criminal fines. Contempt of a decision issued by the FDPIC also can result in criminal fines.

The criminal fines may be as high as CHF 250,000.00.

In principle, these fines would be levied against the individual responsible for making the decision resulting in the violation (and not the company itself), such as the head of HR.

Contact persons

Simone Wetzstein
Partner, Zurich
Phone +41 58 658 56 54
simone.wetzstein@walderwyss.com

Irène Suter-Sieber
Partner, Zurich
Phone +41 58 658 56 60
irene.suter@walderwyss.com

Philippe Nordmann
Partner, Basel
Phone +41 58 658 14 50
philippe.nordmann@walderwyss.com

Rayan Houdrouge
Partner, Geneva
Phone +41 58 658 30 90
rayan.houdrouge@walderwyss.com

Stefano Fornara
Partner, Lugano
Phone +41 58 658 44 23
stefano.fornara@walderwyss.com

Olivier Sigg
Partner, Geneva
Phone +41 58 658 30 20
olivier.sigg@walderwyss.com

Fabian Looser
Counsel, Basel
Phone +41 58 658 14 61
fabian.loser@walderwyss.com

Laura Luongo
Counsel, Geneva
Phone +41 58 658 30 21
laura.luongo@walderwyss.com

Alex Domeniconi
Managing Associate, Lugano
Phone +41 58 658 44 06
alex.domeniconi@walderwyss.com

Jonas Knechtli
Managing Associate, Basel
Phone +41 58 658 14 82
jonas.knechtli@walderwyss.com

Yannik A. Moser
Managing Associate, Basel
Phone +41 58 658 14 85
yannik.moser@walderwyss.com

Sandrine Kreiner
Senior Associate, Geneva
Phone +41 58 658 30 89
sandrine.kreiner@walderwyss.com

Flora V. Francioli
Senior Associate, Lausanne
Phone +41 58 658 83 79
flora.francioli@walderwyss.com

Christoph Burckhardt
Associate, Basel
Phone +41 58 658 14 34
christoph.burckhardt@walderwyss.com

Bertrand Donzé
Associate, Geneva
Phone +41 58 658 30 92
bertrand.donze@walderwyss.com

Valentina Eichin
Associate, Zurich
Phone +41 58 658 52 76
valentina.eichin@walderwyss.com

Contact persons

Martin Greuter
Associate, Zurich
Phone +41 58 658 51 43
martin.greuter@walderwyss.com

Tabea Gutmann
Associate, Zurich
Phone +41 58 658 57 90
tabea.gutmann@walderwyss.com

Gustaf Heintz
Associate, Zurich
Phone +41 58 658 57 30
gustaf.heintz@walderwyss.com

Kathryn Kruglak
Associate, Geneva
Phone +41 58 658 30 91
kathryn.kruglak@walderwyss.com

Nadja D. Leuthardt
Associate, Basel
Phone +41 58 658 14 62
nadja.leuthardt@walderwyss.com

Bojan Momic
Associate, Basel
Phone +41 58 658 14 47
bojan.momic@walderwyss.com

Angelina Pellegrini
Associate, Zurich
Phone +41 58 658 58 68
angelina.pellegrini@walderwyss.com

Patricia Pinto
Associate, Geneva
Phone +41 58 658 30 86
patricia.pinto@walderwyss.com

Michelle Sollberger
Associate, Berne
Phone +41 58 658 29 23
michelle.sollberger@walderwyss.com

Céline Squaratti
Associate, Zurich
Phone +41 58 658 30 23
celine.squaratti@walderwyss.com

Stephanie Wichmann
Associate, Zurich
Phone +41 58 658 52 42
stephanie.wichmann@walderwyss.com

Chiara Wirz
Associate, Zurich
Phone +41 58 658 52 46
chiara.wirz@walderwyss.com