



New Federal Act on Data Protection (FADP) | Comparison to the GDPR

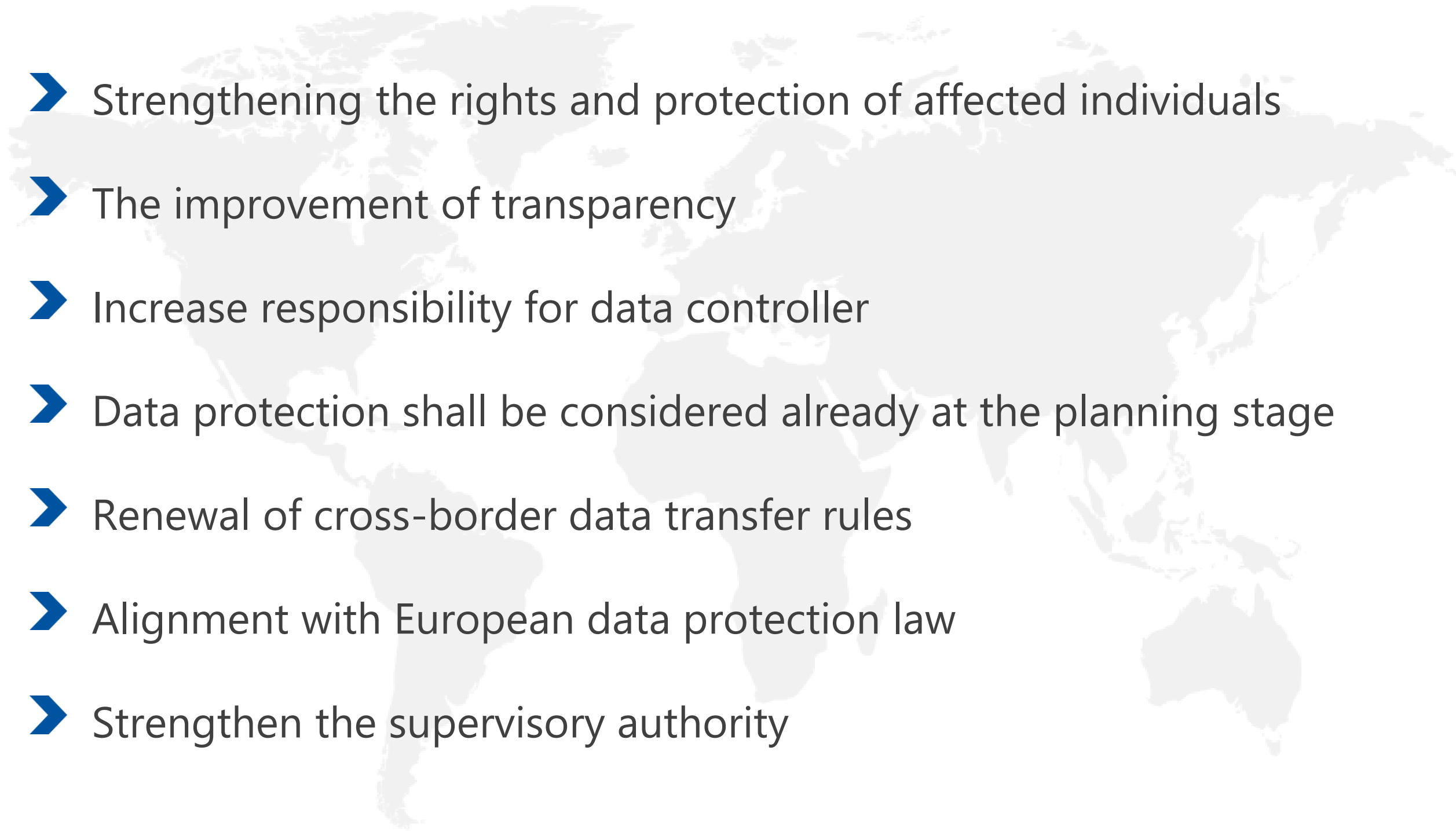
Yves Gogniat

Attorney-at-Law, LL.M., CIPP/E, CIPP/A | Partner at Wicki Partners AG

Reasons and Goals of the Revision I

- The Federal Act on Data Protection (FADP) had been introduced in 1992
- Technological progress
- EU has a strict and modern data protection law since 2018
- Switzerland has signed the Council of Europe's Data Protection Convention 108
- Switzerland aims for equivalence with EU data protection law

Reasons and Goals of the Revision II

- 
- Strengthening the rights and protection of affected individuals
 - The improvement of transparency
 - Increase responsibility for data controller
 - Data protection shall be considered already at the planning stage
 - Renewal of cross-border data transfer rules
 - Alignment with European data protection law
 - Strengthen the supervisory authority

Comparison I

➤ Material scope:

- Material scope: Similar, however, FADP is even a bit broader as it does not mention; "processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."
- Only natural persons are in scope (legal entities are no longer in scope)
- The definition of sensitive personal data will explicitly include biometric and genetic data

➤ Territorial scope of application:

- The law applies to data processing that have an effect in Switzerland, even if they are the processing is abroad.

➤ Alignment with the GDPR

➤ Do we need a representative now (similar art. 27 GDPR)?

- According to Article 14 FADP Controllers/Processors without a registered office in Switzerland have to designate a representative in Switzerland if:
 - They process personal data of persons in Switzerland;
 - this obligation is triggered if the data processing is connected with the offering of goods or services or the observation of the behavior of these persons;
 - and if the processing entails **a high risk for the data subject** concerned.

Comparison II

- **Processing of personal data (article 30 and 31 nFADP)**
- FADP = Permission with reservation of prohibition: Justification only necessary if data processing is illegal vs. GDPR = Prohibited without a justification.
- Data processing is unlawful if data are processed contrary to the basic principles, if the data subject has expressly objected to data processing or if personal data that are particularly sensitive are disclosed to third parties.
- **FADP leaves the controller more flexibility**
- The notion of **high-risk profiling** was introduced – Consent for high-risk profiling has to be explicit

Comparison III

- **Extended information requirements;** including details of the responsible person, the purpose of processing and the categories of recipients (exceptions in the case of disproportionate effort to obtain information [third-party procurement])
- Generally less extensive requirements than under GDPR
- One potentially burdensome deviate form GDPR:
 - Swiss law provides for more extensive disclosure when data is transferred abroad.
 - "If the personal data is disclosed abroad, the data subject shall also be informed **of the country or international body** and, where appropriate, of the guarantees referred to in Article 13, paragraph 2, or of the application of an exception under Article 14."

Comparison IV

- **Automated individual decision-making**
- **Data Protection Impact Assessment**
 - If the risk is high, an opinion of the supervisory authority must be obtained. However, if a data protection advisor has been appointed, no opinion needs to be obtained.
- **Privacy by Design and Privacy by Default**
- **No Data Protection Officer necessary**
- **Instead of a DPO; Data protection advisor** (voluntary but has advantages)

Comparison V

- **Records of processing activities**
- **Exception:** The Federal Council will provide exceptions for enterprises that employ fewer than 250 employees and whose data processing involves only a low risk of a privacy violation.
- We will have to wait for the Data Protection Ordinance for more clarity
- **Data Breach Notification**
 - Timeline ASAP (in practice it will be probably similar to the GDPR. However, the Swiss rule leaves more room for interpretation).
 - Nature of breach should be included, consequences and measures to react against the breach
 - Informing Swiss supervisory authority
 - Only when appropriate and necessary the data subjects have to be informed

Comparison VI

➤ Data Processor

- FADP uses a similar definition
- The processing of personal data may be entrusted by contract or by law to a data processor if the data is processed in the way in which the data controller is entitled to do so, and no legal or contractual obligation of confidentiality prohibits the transfer.
- Sub-delegation requires consent
- A contractual agreement between the controller and the processor is usually required, but this arrangement must not be as detailed as under GDPR.
- As a minimal requirement the controller needs to ensure that a processor has sufficient **technical and organizational measures** in place and that data is only processed in the way in which the data controller is entitled to do so itself.

Comparison VII

➤ International Data Transfer

- Both laws provide for similar regulations.
- A distinction is made between countries with an adequate level and those without (third countries). In the case of third countries, comparable mechanisms (standard contractual clauses, BCRs, etc.) or legal grounds (e.g., contractual handling) can be used.

Comparison VIII

➤ Data Subject Rights

- The data subject has a right to his information/access;
- a right of correction (with exceptions);
- and a right of portability.
- The remaining rights (in particular the right to deletion) are not explicitly mentioned in the FADP but arise indirectly from the FADP (article 32 nFADP) or are otherwise regulated in the legal system (e.g. privacy actions according to Art. 28 CC).

➤ Less comprehensive than GDPR

Fines

- **Administrative Fines:** The Federal Data Protection and Information Commissioner ("FDPIC") will have the competence to issue orders, but not to issue fines directly (unlike under the GDPR).
 - Failure to comply with an order may lead to criminal proceedings and a fine of up to CHF 250,000.00
- **Criminal Fines** (with intent / conditional intent): Up to a CHF 250,000 fine.
 - Generally criminal proceedings are always directed against the responsible natural persons and not against a company. Criminal proceedings would therefore be initiated against the management and not only against the company.
 - In the event a fine would not exceed CHF 50,000.00, and the investigation of the offenders would require investigative measures that would be disproportionate to the penalty imposed, the prosecutor may refrain from prosecuting these persons and, in their place, order the company to pay the fine.

Summary / Minimal Compliance

- Review Privacy Policy
- Records of processing activities
- Organizational and technological measures (TOM) = Description Data security
- Review of contracts with processors (sufficient contract clause)
- Information process (IT infrastructure check)
- Process for data breach
- Review international data transfer
- Privacy Impact Assessment Process
- **Minimal compliance is necessary to avoid intentionally violating the regulations and becoming liable under criminal law.**

THANK
YOU!