

Your World First

C/M/S/

Law . Tax

**Newsletter**

July 2017

---

## The new data protection law – main changes at a glance

Overview of the main differences between the General Data Protection Regulation (GDPR), the Swiss Federal Act on Data Protection (FADP) and the pre-draft of the new Swiss Federal Act on Data Protection in direct comparison

July 2017

---

# The new data protection law: new challenges for companies

After years without any substantial changes, the data protection law, against the backdrop of technological and social changes, now faces a radical transformation – both within the EU and in Switzerland.

## The new EU General Data Protection Regulation

Unlike the previous EU Data Protection Directive 95/46/EC, the new EU General Data Protection Regulation immediately takes effect in all 28 EU member states, becoming applicable as of 25 May 2018. This new law enhances the transparency of data processing and expands the rights of the persons concerned. Additionally, infringements will be sanctioned by substantial penalties.

## Significance for Switzerland

Not only does the EU General Data Protection Regulation apply to EU-based companies; it also directly affects foreign companies whose offer is aimed at a certain national market in the EU, or whose data processing serves to observe the behavior of persons in the EU.

Switzerland will align with the EU General Data Protection Regulation, with the objective of, inter alia, again receiving an adequacy decision from the European Commission, paving the way for trans-border data flows with the EU.

## Revision of the Swiss Federal Act on Data Protection

In view of the new data protection law in the EU, the Swiss Federal Act on Data Protection is also being revised. On 21 December 2016, the Swiss Federal Council submitted the draft bill for consultation.

This publication provides a first overview of the key changes of the new data protection law – through a direct comparison between the new EU General Data Protection Regulation, the currently applicable Swiss Federal Act on Data Protection, and the preliminary draft for the new Swiss Federal Act on Data Protection.



CMS Switzerland

**Caroline Gaul, LL.M.**

Attorney at Law

Member of the German Bar Association  
Frankfurt am Main

Registered in the Swiss roll of solicitors in  
accordance with Art. 28 BGFA

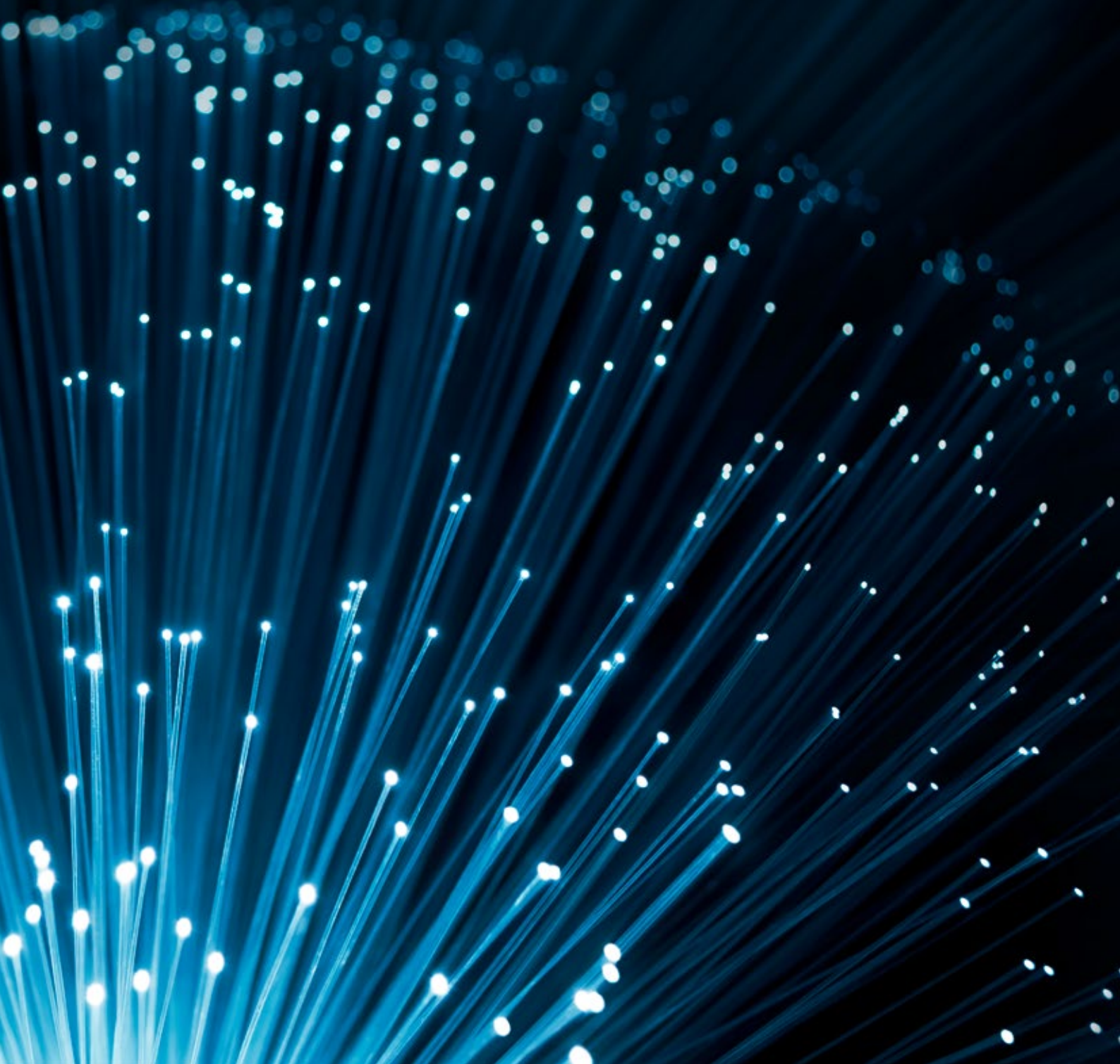
**T** +41 44 285 11 11

**E** caroline.gaul@cms-vep.com



---

Overview of the main differences between the General Data Protection Regulation (GDPR), the Swiss Federal Act on Data Protection (FADP) and the pre-draft of the new Swiss Federal Act on Data Protection in direct comparison



---

## GDPR

---

### Background:

The new GDPR will replace the Data Protection Directive (95/46/EC). Unlike the current Directive, it will be directly applicable in all EU Member States without the need for national legislation. However, a number of “opening clauses” will provide the Member States with flexibility for national implementation (e.g. regarding employee’s personal data in the employment context, designation of data protection officer).

The GDPR will apply from 25 May 2018.

---

### Territorial scope:

Even companies located outside of the EU will be required to comply with the GDPR if their processing is related to:

- the offering of goods or services (free of charge or paid for) to individuals in the EU; or the monitoring of the behaviour of individuals in the EU.
- Indications for “EU-related offerings”: The language of a website alone might not be enough, but the combination of language and currency or the mentioning of EU-based customers/users as a reference.

In case companies located outside the EU are subject to the GDPR, they have an obligation to appoint an EU-based representative. Exemptions apply (i.e. only occasional processing of non-sensitive personal data). The appointment of a representative does not exclude liability of the data controller or data processor.

## Swiss Federal Act on Data Protection (FADP)

---

### Background:

The current FADP has remained largely unchanged since 1993. Presently, the FADP (still) guarantees an “adequate level of protection”, so that personal data may be transferred from the EU to Switzerland and vice versa.

---

### Territorial scope:

**Public law provisions:** principle of territoriality;

**Private law provisions:** according to Art. 139 of the International Private Law Act: upon discretion of the data subject:  
(1) place of the data subject or  
(2) place of the effect of the breach or  
(3) place of the infringer

## Swiss Pre-Draft of the new FADP

---

### Background:

The pre-draft adapts considerably to the GDPR, inter alia in order to (again) achieve an “adequate level of protection” – decision of the European Commission in 2018.

---

### Territorial scope:

**Public law provisions:** principle of territoriality;

**Private law provisions:** according to Art. 139 of the International Private Law Act: upon discretion of the data subject:  
(1) place of the data subject or  
(2) place of the effect of the breach or  
(3) place of the infringer

---

## GDPR

---

**Personal scope:**

Personal data of legal persons is not protected.

---

**Duty to provide information / Privacy notices:**

The GDPR sets a higher standard of notice by adding a significant number of prescribed new fields of information which must be provided proactively (e.g. the period for which the data will be stored, the existence of various data subject rights, the legal basis for the processing, the existence of automated decision making).

Form: No formal requirement but the information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language (the information may be provided in combination with standardised icons).

---

**Access right:**

Any person has the right to access personal data which has been collected concerning him or her. A significant set of information must be provided. Accessing personal data is free of charge; however, any further copies requested by the data subject may incur a reasonable fee based on administrative costs.

## Swiss Federal Act on Data Protection (FADP)

---

**Personal scope:**

Personal data of legal persons is protected.

---

**Duty to provide information / Privacy notices:**

No comparable duty to provide information proactively.

Only a rather modest duty to notify the data subject at the time of the collection of sensitive personal data or personality profiles and (only) of the following: the controller of the data file, the purpose of the processing and the categories of data recipients if a disclosure of data is planned.

---

**Access right:**

Modest duty to provide information upon request (which data, available information on the source of the data, purpose, legal basis, categories of the personal data processed, the other parties involved with the file and the data recipient). In principle free of charge but exceptions apply.

## Swiss Pre-Draft of the new FADP

---

**Personal scope:**

Personal data of legal persons is not protected (anymore).

---

**Duty to provide information / Privacy notices:**

Greater duty to provide information proactively and not only in cases of the collection of sensitive personal data or personality profiles.

Scope: The standard of notice is not as high and detailed as in the GDPR: the data controller shall (only) provide all information which is required in order to enable the data subject to assert its rights according to the FADP and to ensure transparent processing of data, in particular: the data controller's identity and contact information, the processed personal data or the categories of the processed personal data, the purpose of the processing, recipients, processor and the existence of automated decision making.

Form: Comparable to the GDPR.

---

**Access right:**

Extended duty to provide information upon request (envisaged period of storage or, if this is not possible, the criteria used to determine such period, the existence of an automated individual decision-making, if data is disclosed to third parties, the recipients or the categories of recipients, if the data is assigned to a processor, the identity and contact information of the processor as well as the data or the categories of data that it processes).

---

## GDPR

---

### Right to data portability:

Right to transmit data to another controller.

---

### Further rights of the data subject:

Right to rectification.

Right to erasure.

Right to restriction of processing.

---

### Data of deceased persons:

The GDPR does not apply to the personal data of deceased persons and does not provide any rules regarding the data of deceased persons.

---

### Cross-border disclosure:

Personal data should not be transferred to a country outside the European Economic Area unless there is an "adequate level of protection" or an exemption applies, in particular, in the case of EU-Model Clauses or Binding Corporate Rules, which are now expressly provided in the GDPR but still must be approved by the relevant supervisory authority.

## Swiss Federal Act on Data Protection (FADP)

---

### Right to data portability:

No right to data portability.

---

### Further rights of the data subject:

Right to rectification.

Right to erasure not explicitly regulated but derives from the right of privacy.

Right to restriction of processing not explicitly regulated but derives from the right of privacy.

---

### Data of deceased persons:

No provisions regarding the data of deceased persons in the FADP (only regarding access to data relating to deceased persons, regulated in the Ordinance to the FADP).

---

### Cross-border disclosure:

Personal data may not be disclosed abroad unless there is an "adequate level of protection" (please see the non-binding list of countries published by the Federal Data Protection and Information Commissioner).

Exemptions apply, in particular in the case of EU-Model Clauses and Binding Corporate Rules, which must be reported to the Federal Data Protection and Information Commissioner. Binding Corporate Rules and those EU-Model Clauses that have been amended might be checked by the Federal Data Protection and Information Commissioner within 30 days.

## Swiss Pre-Draft of the new FADP

---

### Right to data portability:

No right to data portability.

Reason: In the view of the Federal Council the right to data portability focuses more on the right of the data subject to receive its data in order to benefit from competition than it focuses on the protection of privacy.

---

### Further rights of the data subject:

Right to rectification.

Right to erasure explicitly regulated.

Right to restriction of processing explicitly regulated.

---

### Data of deceased persons:

Provisions regarding the data of deceased persons ("digital death").

---

### Cross-border disclosure:

Personal data may not be disclosed abroad unless there is an "adequate level of protection". New: the Federal Council determines whether the legislation of a state guarantees adequate level of protection.

Exemptions apply, in particular in case of (EU-)Model Clauses, which were previously approved by the Federal Data Protection and Information Commissioner, or which the Commissioner has issued or recognised and in case of Binding Corporate Rules which (new!) may also previously be approved by a foreign authority which is responsible for data protection and which belongs to a state which guarantees adequate protection.







---

## GDPR

---

### Impact of the European Data Protection Board:

The European Data Protection Board shall ensure the consistent application of the GDPR, it shall, in particular: issue guidelines, recommendations and best practices. It is composed of the head of one supervisory authority of each member state and of the European Data Protection Supervisor.

---

### Automated individual decision-making:

Automated individual decision-making which produces legal effects on the data subject or similarly significantly affects him or her is prohibited.

Example: automated refusal of an online credit application.

Exemptions apply if the decision:  
(1) is necessary for the contract; or  
(2) is authorised by Union or Member State law; or  
(3) is based on the data subject's explicit consent.

---

### Data protection impact assessment:

The GDPR places an obligation on data controllers to perform an impact assessment where, taking into account the nature, scope, context and purposes of the processing, is likely a high risk to the rights and freedoms of individuals.

Where a data protection impact assessment indicates that the processing would still result in a high risk, the data controller shall consult the supervisory authority prior to processing.

---

## Swiss Federal Act on Data Protection (FADP)

---

### Impact of the Federal Data Protection and Information Commissioner:

Recommendations.

---

### Automated individual decision-making:

Automated individual decision-making is not prohibited.

---

### No data protection impact assessment

---

## Swiss Pre-Draft of the new FADP

---

### Impact of the Federal Data Protection and Information Commissioner:

“Good practice recommendations”: Compliance with the good practice recommendations means compliance with the data protection provisions that are specified by the good practice recommendations.

---

### Automated individual decision-making:

Automated individual decision-making is not prohibited but triggers a duty of information.

Furthermore: The data subject has the opportunity to comment on the automated individual decision and the processed personal data. The duty of information and consultation does not apply when an automated individual decision is provided for in a formal law.

---

### Data protection impact assessment:

The data controller or the data processor must conduct a data protection impact assessment in advance and notify the Federal Data Protection and Information Commissioner of the outcome of the data protection impact assessment.

The Federal Data Protection and Information Commissioner already offers an “App” for the data protection impact assessment: <https://www.apps.edoeb.admin.ch/dsfa/de/index.html>

---



---

## GDPR

---

### Data breach reporting:

The GDPR introduces a system of mandatory notification for data breaches. Data controllers will be required to notify personal data breaches to supervisory authorities without undue delay and, where feasible, no later than 72 hours of becoming aware of the breach. Set categories of information must be provided in the notification. However, there will be a materiality threshold whereby notification to supervisory authorities is not required if the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Data controllers must also communicate data breaches to data subjects without undue delay, although, this is only required when the breach is likely to result in a risk to the rights and freedoms of individuals.

---

### Privacy by Design and Privacy by Default:

Implementation and specification of the principles of data avoidance and data economy:

Privacy by design = data protection by implementation of technical and organisational measures into the processing, e.g. pseudonymisation.

Privacy by default = data protection by implementing measures to ensure that, by default, only personal data necessary for the specific purpose of the processing are indeed processed. This involves the restriction of personal data collected, the period of storage of the personal data and their access.

## Swiss Federal Act on Data Protection (FADP)

---

### No data breach reporting

---

### Privacy by Design and Privacy by Default:

No specific formal law other than the "principle of proportionality".

## Swiss Pre-Draft of the new FADP

---

### Data breach reporting:

The controller must notify the Federal Data Protection and Information Commissioner without undue delay of an unlawful processing of data or loss of data unless the breach of data protection is unlikely to result in a risk to the privacy or the fundamental rights of the data subject.

Data controllers must also communicate data breaches to data subjects if this is necessary for the protection of the data subject or the Commissioner requests so.

The register of data files will be abolished.

---

### Privacy by Design and Privacy by Default:

The principles of privacy by design and privacy by default are implemented into law.

---

## GDPR

---

### Records of processing:

Under current data protection law, data controllers in all EU Members States must, subject to some limited exemptions, notify the relevant national data protection authority of their processing activities. The GDPR abolishes current notification requirements and instead requires both data controllers and data processors to keep relatively detailed records of their processing activities and make these available to supervisory authorities on request. There is an exemption for enterprises or organisations that employ fewer than 250 persons unless the processing is high risk, not occasional, or includes “special categories of data” and/or personal data relating to criminal convictions and offences (which in general terms is “special categories of data” under the Directive, plus new categories of genetic and biometric data).

---

### Data protection officers:

Data controllers and processors have a duty to designate a data protection officer if required under national law or if their core activities involve either the regular, systematic and large scale monitoring of individuals or the large scale processing of “special categories of data” and/or “personal data relating to criminal convictions and offences”.

---

### Supervisory authority with extensive power:

Issue warnings and reprimands, order compliance, impose a temporary or definitive limitation including a ban on processing, impose an administrative fine, order provisional measures, bring infringements to the attention of the judicial authorities and to commence or engage in legal proceedings.

## Swiss Federal Act on Data Protection (FADP)

---

### No records of processing:

No duty to keep records of all processing activities but a registration requirement in limited cases resulting in a duty to maintain records and to issue a processing policy.

---

### Data protection officers:

No duty to designate a data protection officer.

---

### The Federal Data Protection and Information Commissioner may:

- make recommendations
- refer the matter to the Federal Administrative Court for a decision
- apply to the Federal Administrative Court for interim measures to be taken

## Swiss Pre-Draft of the new FADP

---

### Records of processing:

Duty to document all data processing. Details will be specified in the Ordinance to the FADP.

The duty to register data files will be abolished.

---

### Data protection officers:

No duty to designate a data protection officer.

---

### The Federal Data Protection and Information Commissioner may:

- order preliminary measures
- order administrative measures (e.g. defer or prohibit disclosure abroad, order destruction of the data)

---

## GDPR

---

### Fines:

The GDPR establishes a two-tiered system of administrative fines, which is applicable to both data controllers and data processors. Some infringements (for example of provisions relating to keeping records of processing) are subject to fines of up to EUR 10.000.000, or for an undertaking, up to 2% of worldwide annual turnover in the previous financial year, whichever is higher. Others (such as breaches of the basic principles for processing/conditions for obtaining consent) are punishable by higher fines of up to EUR 20.000.000, or for undertakings, up to 4% of worldwide annual turnover in the previous financial year, whichever is higher.

## Swiss Federal Act on Data Protection (FADP)

---

### Fines:

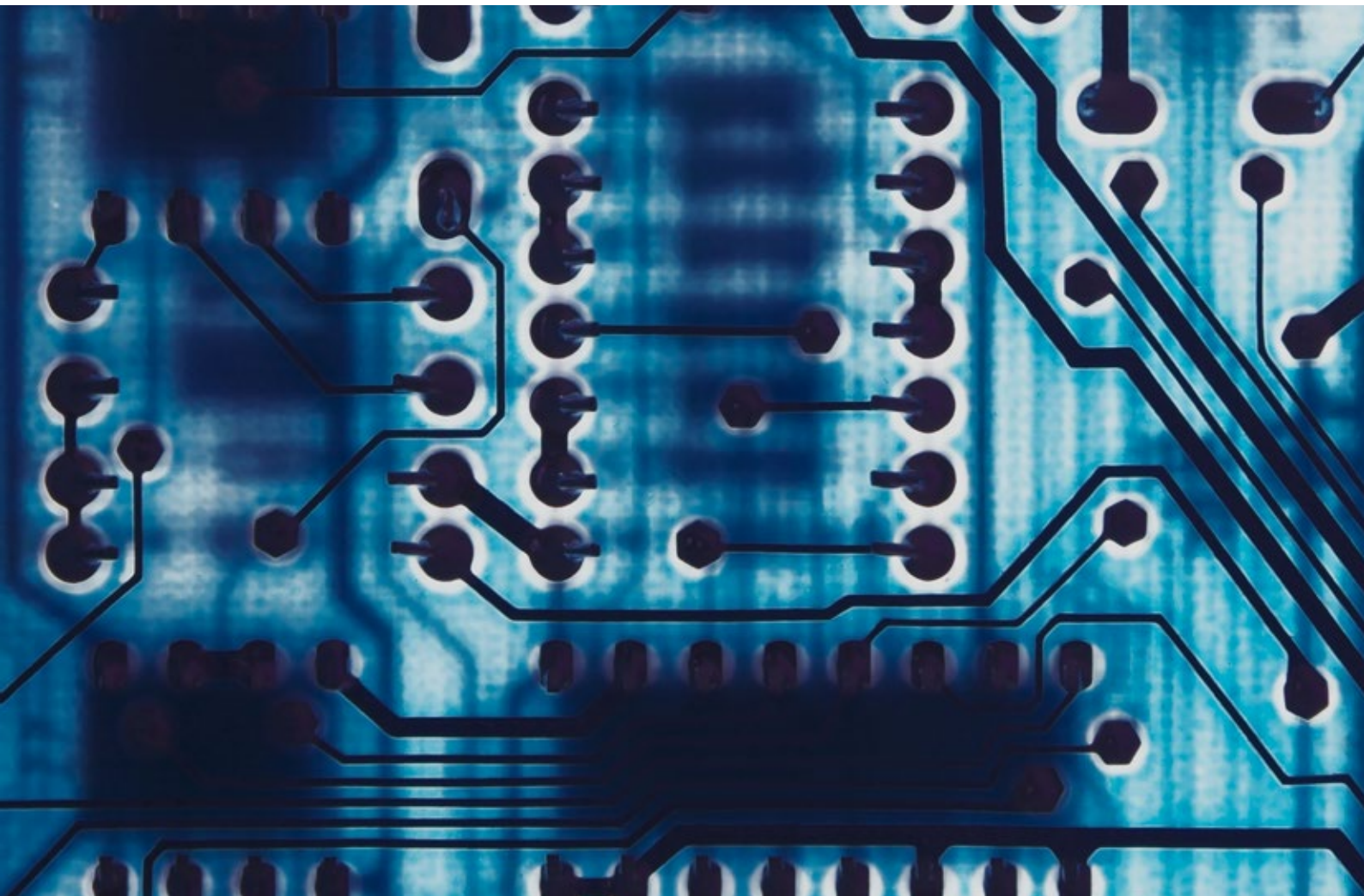
Liability to a fine of (only) up to 10.000 Swiss Francs, only in a very limited number of cases and only upon complaint.

## Swiss Pre-Draft of the new FADP

---

### Fines:

Fines of up to 250.000 Swiss Francs for a negligent breach and fines of up to 500.000 Swiss Francs for an intentional breach. If the fine does not exceed 100.000 Swiss Francs and it appears that the investigation into punishable persons requires criminal investigation measures which would be disproportionate to a potential sentence, the authority may decide not to prosecute these persons and instead sentence the undertaking to the payment of the fine.







**Your free online legal information service.**

A subscription service for legal articles on a variety of topics delivered by email.  
**[cms-lawnow.com](http://cms-lawnow.com)**



**Your expert legal publications online.**

In-depth international legal research and insights that can be personalised.  
**[eguides.cmslegal.com](http://eguides.cmslegal.com)**

---

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices.

**CMS locations:**

Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luxembourg, Lyon, Madrid, Manchester, Medellín, Mexico City, Milan, Monaco, Moscow, Munich, Muscat, Paris, Podgorica, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sheffield, Singapore, Sofia, Strasbourg, Stuttgart, Tehran, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

---

**[cms.law](http://cms.law)**