May 26, 2021

Developments in UK and Swiss Data Protection Law

Juliette Hotz
Swisscom (Switzerland) AG

Sarah Pearce
Paul Hastings LLP

Thomas Steiner
LAUX LAWYERS AG

Privacy+ Security Forum

Agenda

- Introduction
- Developments in Swiss Data Protection Law
- Developments in UK Data Protection Law
- Take-aways

Introduction

Privacy+ Security Forum

Speaker

Privacy+ Security Forum

Juliette Hotz

Senior Counsel, Data Governance
Swisscom (Switzerland) AG (Zurich)

- Senior Legal Counsel with a focus on data protection in the IT and telecom industries
- Managed GDPR implementation project for Swisscom's enterprise customers business
- Manages (revised) Swiss FADP implementation project at Swisscom

Speaker

Sarah Pearce

Partner, Paul Hastings LLP (London and Paris)

- Heads Paul Hastings' European Data Privacy and Cybersecurity team
- Focus on data privacy and security issues in the UK and across Europe, including the impact of Brexit and the aftermath from the UK leaving the EU

Speaker

Thomas Steiner

Partner, LAUX LAWYERS AG (Zurich)

- Data, privacy and technology lawyer
- Actively involved in revision of Swiss FADP
- Supports Swiss and international companies in implementing compliance with Swiss FADP (and EU GDPR)

Disclaimer

Our opinions are our own and not those of our firms, companies, or clients.

Purposes & Goals

- Learn how Swiss and UK data protection laws compare to the EU GDPR
- Offer practical compliance tips regarding the implementation of the requirements of Swiss and UK laws in companies with data protection programs that are benchmarked on the GDPR
- Best practices for multinational clients doing business in Switzerland or the UK

Developments in Swiss Data Protection Law

Privacy+ Security Forum

Overview

1. When and why a revised Swiss Federal Act on Data Protection

2. How the revised FADP compares to the GDPR, with a focus on
   - Transparency
   - Right of Access
   - International Data Transfers

3. Practical tips for operationalization of compliance

Revised FADP

- Revised FADP adopted in final vote of Federal Parliament on September 25, 2020
- Key objectives: implement **revised Council of Europe Convention 108** and **align** FADP **with the EU GDPR**
- Federal Department of Justice is drafting revised Ordinance on FADP (Revised FODP)
- Revised FODP open for comments starting June 2021 entry info force in the course of **2022**
- Applicable from entry into force – **no transition period!**

Conceptual differences

- **EU GDPR**: The default rule is “prohibited”
  - Companies need a **legal basis** (“good reason”) in order to lawfully process personal data
  - Companies need to actively **inform** individuals (data subjects) on legal bases relied on, and to document their choice of legal bases

- **Swiss FADP**: The default rule is “allowed”
  - Private organizations are generally **allowed** to process personal data if they comply with the **data processing principles**
  - Companies need a **basis for justification** of otherwise unlawful **personality rights infringements** (e.g., disclosure of sensitive personal data to other controllers or continued processing despite the data subject’s explicit objection)

Revised FADP: Aligned with GDPR

Privacy+ Security Forum

Fed. Agencies: Legal Basis
(**Private organizations**: basis for justification, where necessary!)

Processing Principles
(lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, accuracy, security)

Transparency
(Duties to inform data subjects; changes to **privacy notices** recommended)

Data Subject Rights
(rights of access and information, **objection**, rectification erasure and data portability, **+ restriction etc.**)

Documentation / Governance

Requirements for Outsourcing of Processing Operations (processing on behalf of controller)

Int'l Data Transfers
(across Swiss border; **list of import countries** required in privacy policy)

Autom. Decision-making, incl. Profiling (right to object) / **high-risk profiling**

Data Protection Impact Assessment / Privacy-by-Design and Default

Data Breach Notification

Data Security

Enforcement

Scope of Revised FADP

Articles 2–3 and 14 Revised FADP

- Personal and material scope: processing of personal data, whether automated or manual
  - by businesses, organizations, or (in the context of business activities only) natural persons
  - by Federal authorities (note: Chapter 6 Revised FADP only applies to processing by Federal authorities)
- Territorial scope
  - Revised FADP covers processing operations with an effect in Switzerland, even if initiated abroad
  - Private International Law Act: Revised FADP applicable if effect on personality rights of data subjects in Switzerland reasonably foreseeable (or choice of law to resolve claim of occurred infringements)

Transparency (1|3)

Article 19 Revised FADP

- **Privacy notices** are **a must** under the Revised FADP
- Shorter list of **minimum elements of information** (Art. 19 para. 2 FADP; comp. Arts 13–14 GDPR)
- “Swiss finish”: Information about data transfers to recipients (controller or processor) outside of Switzerland requires information on the import **countries** and, where applicable, reference to **safeguards** or **derogations** relied on for the data transfer
- **Potential conflict** with GDPR requirement to inform about legal basis since no such requirement applies under Revised FADP

Transparency (2|3)

Article 19 Revised FADP

- **Additional information**, *as far as necessary for exercising data subject rights and for transparent processing* (Art. 19 para. 2 Revised FADP)
  - may require types of information listed in Art. 13 para. 2 (or 14 para. 2) GDPR; and
  - Information about existence of **high-risk profiling**
- **Supplementary**, where applicable, and if not published elsewhere
  - the contact details of the **data protection advisor** – DPO (Art. 10 para. 3 let. d Revised FADP)
  - the name and address of the **Swiss representative** (Art. 14 para. 3 Revised FADP); and
  - the existence of **automated individual decision-making** (Art. 21 para. 1 Revised FADP)

Transparency (3|3)

Privacy+ Security Forum

Article 19 Revised FADP

→ **Practical tips for changes to privacy notices**

- Add list of import countries – more pragmatic and acceptable: indicate geographic **region**
- Indicate **safeguards** or **derogations** relied on for data transfers
- Inform about existence of **high-risk profiling**
- Refer to “applicable data protection laws” rather than GDPR or Swiss FADP provisions
- State that your determination of legal bases applies **to the extent applicable law (such as GDPR) so requires**; to that end, consider including all your legal bases information in one paragraph only (rather than meticulously mapping legal bases with specific purposes or processing operations)

Right of Access (1|2)

Article 25 Revised FADP

- Includes a right to receive a **copy** (e.g., a print-out or extract of a data set) of the personal data undergoing processing (Art. 25 para. 2 let. b Revised FADP; similar to Art. 15 para. 3 GDPR)
- Similar list of minimum elements of information (Art. 25 para. 2 Revised FADP ; comp. Art. 15 GDPR)
- **Additional information**, *as far as necessary for exercising data subject rights and for transparent processing* (Art. 25 para. 2 FADP)
- **30-day** deadline for (first) response
- **Fewer exceptions** than right of access under GDPR (or Art. 23 GDPR-restrictions in Member State laws) – e.g., weak protection of controller's business secrets (Art. 25 Revised FADP)

Right of Access (2|2)

Privacy+ Security Forum

Article 25–26 Revised FADP

→ Practical tips for operationalization of compliance

- Amend your **internal procedures and standard responses** to reflect that **fewer exceptions or restrictions** apply – prevailing interests of third parties, incl. other data subjects or customers; prescribed by law, protection of professional secrecy; **but**: prevailing interests of the controller only if controller does not disclose the personal data to third parties
- **Structure your customer data** in ways that will allow you to provide copies / **extracts** of personal data (e.g., in Excel) without having to disclose sensitive or confidential business information about your company or customers; and without having to redact personal data of other data subjects
- As regards rather **complex requests**, consider implementing a process for **staggered responses**; with first response, submit copies of personal data which are likely most relevant and provide examples of other types of personal data that you will compile and provide upon further request

Int'l Data Transfers (1|2)

Article 16–17 Revised FADP

- Same concept as Arts 44 et seq. GDPR
- Transfers of personal data from Switzerland to recipients in other countries allowed
  - based on adequacy decision by Swiss Federal Council;
  - subject to appropriate safeguards (e.g., Standard Contractual Clauses or Binding Corporate Rules); or
  - derogations for specific situations

Int'l Data Transfers (2|2)

Article 16–17 Revised FADP

→ Practical tips for operationalization of compliance

- Perform (internal and external) **fact-finding**, e.g., based on questionnaires or checklists, to identify data transfers from Switzerland to other countries (and onward transfers)
- Absent adequacy decision by Federal Council, implement safeguards or determine derogations
- Perform data transfer **risk assessment**
- Use EU Standard Contractual Clauses also for purposes of Art. 16 FADP; make sure "Swiss data protection law" is included in definition of applicable data protection law (note: Revised FADP is not a law implementing or supplementing GDPR)

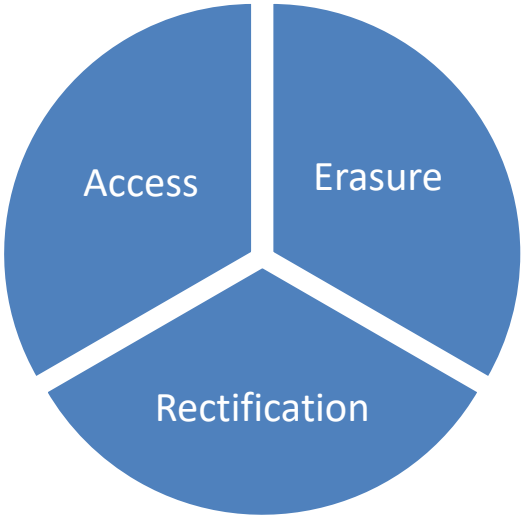
Developments in UK/EU Data Protection Law

Privacy+ Security Forum

Data Subject Rights

GDPR provides a data subject with the following rights:

- To be informed
- To access
- To rectification
- To erasure
- To restrict processing
- To data portability
- Object to processing



Transparency requirements – GDPR and UK GDPR

→ Controllers can satisfy many transparency obligations with a privacy policy

- Information about the processing of a patient's personal data must be easily accessible and easy for them to understand.
- Data subjects must be provided with certain information in relation to the processing of their data such as the identity of the controller, the DPO contract details and the purpose of the processing.
- Information must be provided at the point of data collection.
- Information should be available to all data subjects including those without internet access. Consider leaflets/posters in waiting areas.

Individual Rights: Right to Access

Article 15 GDPR provides the data subject with the right to gain access to the data from the controller

Considerations	
Method of request	The request can be made orally or in writing
Training	Are staff trained to recognise an access request?
Policy	Does the provider have an access to records policy?
Timing	The provider must respond to the request within 1 month. This can be extended by 2 further months where necessary

Individual Rights: Right to Erasure

Article 17 GDPR provides the data subject with the right to be forgotten by the controller

Considerations	
Absolute	The right to be forgotten is not absolute
Is the data necessary?	If the data is necessary for, amongst other purposes, preventative medicine, medical diagnosis or treatment, the data is exempt from Art 17
Public Interest	If the processing is necessary for reasons of public health such as protecting against cross-border threats to health (such as COVID-19) again, the data is exempt

Individual Rights: Right to Rectification

Article 16 GDPR provides the data subject with the right to rectify inaccurate personal data held by the controller

Considerations	
Opinion	Clinical opinion is not inaccurate data, even if it later turns out to be incorrect
Refusal	If a request for rectification is refused, you must explain why and inform the data subject of their right to complain to the relevant regulatory authority

Schrems II – The Remaking of Cross-Border Data Transfers

Privacy+ Security Forum

- **Invalidation of Privacy Shield**. In July 2020, the Court of Justice of the European Union (CJEU) issued its decision in the case *Data Protection Commission v. Facebook Ireland, Schrems (Schrems II)* resulting in the invalidation of the EU-US Privacy Shield Framework.

- **Standard Contractual Clauses Alone May Not be Adequate.** Although the CJEU reaffirmed the validity of Standard Contractual Clauses (SCCs), the court stated that Data Exporters must verify, *on a case-by-case basis*, whether the SCCs alone provide adequate protection. To the extent additional protection is required for the transfer of data to a third country from the EEA, Data Exporters must implement additional safeguards.

- **Technical Measures – A Required Supplemental Measure for US Companies.** The CJEU *in Schrems II*, as well the European Data Protection Board (EDPB) in guidance published in November 2020, both emphasized the need for SCCs be supplemented with technical measures that can ensure a "level of protection essentially equivalent" to that guaranteed in Europe.

- **New Draft Standard Contractual Clauses:** Also in November 2020, the European Commission introduced draft SCCs for public comment. The draft SCCs attempted to address many of the concerns stemming from Schrems II, as well as provide more flexibility for different types of data transfers (e.g., Controller-to-Controller, Controller-to-Processor, Processor-to-Processor, and Processor-to-Controller).

International Transfers: Six-Step Implementation

Overview of EDPB Recommendations and SCC Requirements:

- Data Mapping and Art. 30 requirements
- Conduct appropriate "Transfer Impact Assessments" for the third country and Data Importer
- Evaluate and implement additional supplementary safeguards – especially technical measures – as needed

Map the Data Transfer

Mapping Requirements. Identify the types of personal data involved in the transfer, the purpose of the transfer, and record and map all transfers to third countries, including with all Controllers, Processors, and Sub-Processors that will receive any EEA personal data.

Practical Considerations

Identify Key Exposure Areas by Developing and Updating Data Inventory and Records of Processing

1. **Establish and Maintain an Inventory of Personal Data.** Companies should document (e.g., through data mapping, records of processing, data inventory, and other procedures) how the personal data is transferred to and from vendors and third parties in and outside of the EEA.

2. **Identify Any Onward Transfers.** The Data Exporter and the Data Importer must collaborate to identify all locations where the personal data may be transferred or stored, including onward transfers to Sub-Processors of the Data Importer. This should include any locations where the Data Importer will transfer the personal data for storage or additional handling by Sub-Processors.

3. **Identify Data Transferred as a Result of Remote Access.** Data Exporters should keep in mind that remote access by any Processor or Controller located in a third country (for example in IT support situations) and/or storage in a cloud located outside the EEA is also considered to be a transfer, and that, when using international cloud infrastructure, the Data Exporter must assess whether the data will be transferred to third countries.

Identify Transfer Mechanisms

Select the appropriate Data Transfer Mechanism. Once all third countries have been identified, including any onward transfers, the Data Exporter must determine which data Transfer Mechanism is appropriate for conducting the transfer.

Practical Considerations

1. **Art. 45 Adequacy Determination.** Where a third country has been deemed adequate no further action is required – countries deemed adequate are limited to: Andorra, Argentina, Canada, Faroe islands, Guernsey, Israel, Isla of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay.

2. **Art. 46 Transfer Mechanisms.** Where a third country has not been deemed to provide adequate protection by the European Commission, the Data Exporter must identify alternative Transfer Mechanisms available under GDPR Art. 46 to complete the transfer, including implementing SCCs. Further analysis, including Transfer Impact Assessments are required where an Art. 46 transfer mechanism is employed.
    - Art. 46 transfer mechanisms include Standard Contractual Clauses, Binding Corporate Rules (BCRs), codes of conduct, certification mechanisms, and ad hoc contractual clauses)

3. **Art. 49 Derogations.** Derogations permitting the transfer of personal data include: consent, performance of a contract, public interest, legal claims, vital interests, and legitimate interests (where adequate notice is provided). Where Art. 49 derogations are the basis of the transfer, no additional analysis is required.

Transfer Impact Assessment – Third Country Privacy Framework

Identification of Third Country Privacy Framework. Where Art. 46 Transfer Mechanisms will be used, the Data Exporter must perform and document a Transfer Impact Assessment (TIA) to determine whether the Transfer Mechanism provides adequate protections for any transferred personal data.

- **Conduct Transfer Impact Assessment.** A Transfer Impact Assessment is a review of the laws and practices of a third country to determine whether transferred personal data would be afforded an equivalent level of protection to that provided in the EEA.
- **Key Criteria.** The primary criteria for assessing a third country's privacy framework are:
  - (1) laws requiring disclosure of personal data to public authorities (e.g., criminal law enforcement, regulatory supervision, and national security agencies); and
  - (2) whether the circumstances surrounding such disclosures can be regarded as a 'justifiable interference' that does not impinge on the transfer safeguards.
- **Third Countries Requiring Careful Review.** Countries with limited or sector-specific privacy legislation or case law should be carefully reviewed against 'objective sources' to determine the actual level of protection; such countries include the United States, Russia, and China.

Practical Considerations

Transfer Impact Assessment – Assessment of the Data Importer

Assess the data handling practices of the Data Importer. The Data Exporter should require the Data Importer to complete a privacy and security evaluation questionnaire. During the evaluation process, the Data Exporter and Data Importer should take into account: (i) the nature of the personal data and (ii) the nature, scope, context, and purposes of processing.

Practical Considerations

The SCCs do not provide prescriptive requirements for security, but advise the parties to the contract to consider establishing requirements for the following security topics:

- Pseudonymization and encryption at rest and in transit
- Maintaining ongoing confidentiality, integrity, availability, and resilience of processing systems
- Data availability, access, and back-up
- Testing and evaluation of technical and organizational measures
- Information security configurations, governance, and management
- Physical security
- Certifications and assurances
- Data avoidance and minimization, and
- Data quality, retention, accountability, portability, and disposal

Supplementary Measures – Assessment and Implementation

Privacy+ Security Forum

Select the Appropriate Supplementary Measures. Supplementary measures should be evaluated on a case-by-case basis with input from both the Data Exporter and the Data Importer. It is expected that supplementary measures are actionable – requiring technical safeguards – and not merely policy.

Three Types of Supplementary Measures.
Supplementary measures fit into 3 main categories:

1. Technical
2. Contractual
3. Organizational

Complimentary Supplementary Measures. There is no exhaustive list of supplementary measures, and the parties may implement complementary layers of supplementary measures in order to attain the necessary level of protection.

- For example – Technical measures can impede, or render ineffective, access to personal data by a third country government, and contractual or organizational measures can supplement technical measures for additional protection.

Practical Considerations

Assessment of Supplementary Measures	Types of Supplementary Measures
Use information collected during TIAs to evaluate whether supplementary measures are technically or operationally feasible. Below is a list of potential considerations: ➢ Format of the data to be transferred (i.e., in plain text/pseudonymised or encrypted) ➢ Nature of the data ➢ Length and complexity of data processing workflow ➢ Possibility that the data may be subject to onward transfers	➢ ***Technical Measures:*** • Encryption at rest and in transit • Client-side encryption with key located in EU • Psuedonymization • Multi-party or multi-channel processing ➢ ***Contractual Measures:*** • Requirements for redress mechanisms and legal counselling • Prohibition against backdoor access • Right to audit • Notice for any onward transfer • Notify Data Exporter of non-compliance or governmental access ➢ ***Organizational Measures:*** • Internal policies with clear allocation of responsibilities, reporting channels, and standard operating procedures for cases of covert or official requests from public authorities to access transferred data.

Brexit

- Key Issues:
  - Distinction between regulation and directive under EU law.
  - GDPR – UK will be a third country
  - Can data flow freely?
  - ePrivacy Regulation

Brexit Data Flow Scenarios

	UK → EU	EU → UK	UK → Adequate	UK → third country
Pre Brexit	Y	Y	Y	N
Post Brexit – No Deal	Y	N	Y	N
Post Brexit – Deal during Transitional Period	Y	Y	Y	N
Post Brexit – Deal after Transitional Period	Y?	Y?	Y?	N

Other Possible Considerations and Effects of Brexit

Pre-Brexit	Post-Brexit
Lead Supervisory Authority • One-Stop-Shop principle • Co-ordinate investigations • Potential controversy	If Lead Supervisory Authority is the ICO (i.e. the UK), this should be **changed to another EU member state.**
Data Protection Officer • To be appointed in certain circumstances • For processing by group companies, one DPO can be appointed	Whilst the UK will no longer be an EU member state, the ICO have confirmed that a DPO acting for UK and EU member state entities can **continue it their role.**
Reporting Personal Data Breaches • Report personal data breach to supervisory authority or lead supervisory authority • Risk to rights and freedoms	If breach affects UK and EU data, **report to both** ICO and member state supervisory authority or lead supervisory authority
EU Representative • Appoint EU representative if subject to Article 3(2) • Often services providers appoint • Cannot be DPO	UK business offering goods or services to EU individuals with **no EU establishment will need to appoint EU representative**
Notice to Data Subjects • Inform data subjects how and why their data is being processed • Privacy policies	**Review and update policies** to reflect any changes to the business such as those above or others

Take-aways

Privacy+ Security Forum

Take-aways

- Switzerland
  - Privacy notices: add list of countries/regions, account for nuances regarding legal bases/justifications
  - Access requests: amend policies and standard responses to reflect limited exceptions
  - Int'l data transfers: perform internal fact-finding re identification of data transfers, import countries and safeguards; implement missing safeguards (such as SCCs)
- UK/EU
  - Transparency: ensure privacy notice is easily accessible and easy to understand
  - Individual Rights: list in privacy notice and ensure policy/procedures in place to comply
  - International Transfer: perform TIA, implement appropriate additional safeguards

Questions + Contact

Juliette Hotz
juliette.hotz@swisscom.com

Sarah Pearce
sarahpearce@paulhastings.com

Thomas Steiner
thomas.steiner@lauxlawyers.ch