FADP revision: comparison to current law and GDPR

This comparison is based on the following laws and regulations:

- Federal Act on Data Protection of 19 June 1992 (FADP, as of 1 March 2019)
- Final vote on the revised FADP of 25 September 2020 (revised FADP)
- Excerpts from the EU General Data Protection Regulation (GDPR, Regulation (EU) 2016/679)

Due to the large number of differences in structure and system and in order to achieve the greatest possible overview, the provisions of the GDPR have been included in the table selectively and, as a rule, in extracts. Direct conclusions regarding the legal situation or the existence or non-existence of regulations should therefore always only be drawn by referring to the complete texts of the individual decrees. The development of the debate on the FADP revision in parliament and the Federal Council's draft can be seen, among other things, in the official "flag" before procedure for reconciling of differences. Further information can also be found on Parliament's "affairs website" and at www.mll-news.com

3 December 2020

Lukas Bühlmann, LL.M.
Partner, Zurich
lukas.buehlmann@mll-legal.com

Dr. Michael Reinle, LL.M.
Partner, Zurich
michael.reinle@mll-legal.com

Meyerlustenberger Lachenal AG, Rechtsanwälte
Schiffbaustrasse 2 | Postfach | 8031 Zürich | Schweiz
T +41 44 396 91 91 | F +41 44 396 91 92
www.mll-legal.com | www.mll-news.com

FADP revision: comparison with current law and the GDPR

revised FADP	FADP	GDPR
Chapter 1: Purpose, Scope and Supervisory Authority of the Confederation		
Art. 1 Purpose This Act aims to protect the personality rights and the fundamental rights of natural persons whose personal data is processed.	**Art. 1 Purpose** This Act aims to protect the privacy and the fundamental rights of persons when their data is processed.	**Art. 1 Subject-matter and objectives** (1) This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. (2) This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. (3) The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.
Art. 2 Personal and material scope [1] This Act applies to the processing of personal data pertaining to natural persons by: a. private persons; b. federal bodies. [2] It does not apply to: a. personal data that is processed by a natural person exclusively for personal use; b. personal data that is processed by the Federal Chambers and parliamentary committees in connection with their deliberations; c. personal data that is processed by institutional beneficiaries according to Article 2 paragraph 1 of the Host State Act of 22 June 2007, which enjoy immunity in Switzerland. [3] The processing of personal data and the rights of the data subjects in court proceedings and proceedings governed by the federal rules of procedure are governed by the applicable procedure law. The present Act applies to first instance administrative proceedings. [4] The public registers pertaining to private law relationships, in particular the access to these registers and the rights of the data subjects, are governed by the special provisions of the applicable federal law. If the special provisions do not contain any rules, this Act shall apply.	**Art. 2 Scope** [1] This Act applies to the processing of data pertaining to natural persons and legal persons by: a. private persons; b. federal bodies. [2] It does not apply to: a. personal data that is processed by a natural person exclusively for personal use and which is not disclosed to outsiders; b. deliberations of the Federal Assembly and in parliamentary committees; c. pending civil proceedings, criminal proceedings, international mutual assistance proceedings and proceedings under constitutional or under administrative law, with the exception of administrative proceedings of first instance; d. public registers based on private law; e. personal data processed by the International Committee of the Red Cross.	**Art. 2 Material scope** (1) This Regulation applies to the 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. (2) This Regulation does not apply to the processing of personal data: a) – b) (…) c) by a natural person in the course of a purely personal or household activity; d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. (3) – (4) (…)
Art. 3 Territorial scope [1] This Act is applicable to fact patterns that have an effect in Switzerland, even if they occurred abroad. [2] The Federal Act of 18 December 1987 on Private International Law applies to claims under civil law. The provisions on the territorial scope of the Swiss Criminal Code remain reserved.		Art. 3 Territorial scope (1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. (2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not

revised FADP	FADP	GDPR
		established in the Union, where the processing activities are related to: a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or b) the monitoring of their behaviour as far as their behaviour takes place within the Union. (3) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.
Art. 4 Federal Data Protection and Information Commissioner [1] The Federal Data Protection and Information Commissioner (FDPIC) supervises the proper application of the federal data protection regulations. [2] The following are excluded from the FDPIC's supervision: a. the Federal Assembly; b. the Federal Council; c. the federal courts; d. the Office of the Attorney General of the Confederation as regards the processing of personal data in criminal proceedings; e. federal authorities as regards the processing of personal data in the context of a jurisdictional activity or of international mutual assistance proceedings in criminal matters.	**Art. 27 Supervision of federal bodies** [1] The Commissioner1 supervises compliance by federal bodies with this Act and other federal data protection regulations of the Confederation. The Federal Council is excluded from such supervision. [2] – [6] (…)	**Art. 51 Supervisory authority** (1) Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority'). (2) – (4) (…) **Art. 55 Competence** (1) – (2) (…) (3) Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.
Chapter 2: General Provisions **Section 1: Definitions and Principles**		
Art. 5 Definitions The following definitions apply in this Act: a. personal data: all information relating to an identified or identifiable natural person; b. data subject: natural person whose personal data is processed; c. sensitive personal data: 1. data on religious, ideological, political or trade union-related views or activities, 2. data on health, the intimate sphere or the racial or ethnic origin, 3. genetic data, 4. biometric data which unequivocally identifies a natural person, 5. data on administrative or criminal proceedings and sanctions, 6. data on social security measures; d. processing: any operation with personal data, irrespective of the means and the procedures applied, and in particular the collection, recording, storage, use, modification, disclosure, archiving, deletion or destruction of data; e. disclosure: transmitting or making personal data accessible; f. profiling: any form of automated processing of personal data consisting of using such data to assess certain personal aspects relating to a natural person, in particular to analyse or predict	**Art. 3 Definitions** The following definitions apply: a. personal data (data): all information relating to an identified or identifiable person; b. data subjects: natural or legal persons whose data is processed; c. sensitive personal data: data on: 1. religious, ideological, political or trade union-related views or activities, 2. health, the intimate sphere or the racial origin, 3. social security measures, 4. administrative or criminal proceedings and sanctions; d. personality profile: a collection of data that permits an assessment of essential characteristics of the personality of a natural person; e. processing: any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data; f. disclosure: making personal data accessible, for example by permitting access, transmission or publication;	**Art. 4 Definitions** For the purposes of this Regulation 1. „ personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; 2. 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; 3. 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future; 4. 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or

revised FADP	FADP	GDPR
aspects relating to that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or whereabouts; g. High risk profiling: profiling which involves a high risk to the personality or fundamental rights of the data subject, as it creates a pairing between data that enables an assessment of essential aspects of the personality of a natural person; h. data security breach: a security breach which leads to an unintentional or unlawful loss, deletion, destruction or modification of personal data or to personal data being disclosed or made accessible to unauthorised persons; i. federal body: federal authority or service or person that is entrusted with federal public tasks; j. controller: private person or federal body that alone or jointly with others decides on the purpose and the means of the processing;, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten;	g. data file: any set of personal data that is structured in such a way that the data is accessible by data subject; h. federal bodies: federal authorities and services as well as persons who are entrusted with federal public tasks; i. controller of the data file: private persons or federal bodies that decide on the purpose and content of a data file; j. formal enactment: 1. federal acts, 2. decrees of international organisations that are binding on Switzerland and international treaties containing legal rules that are approved by the Federal Assembly;	predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; 5. – 6. (…) 7. 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; 8. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; 9. – 26 (…) **Art. 9 Processing of special categories of personal data** (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. (2) – (4) (…)
Art. 6 Principles [1] Personal data must be processed lawfully. [2] Processing must be carried out in good faith and must be proportionate. [3] Personal data may only be collected for a specific purpose which is evident to the data subject; personal data may only be processed in a way that is compatible with such purpose. [4] It is destroyed or anonymized as soon as it is no longer needed with regard to the purpose of the processing. [5] Anyone who processes personal data must ascertain that the data is accurate. He must take all appropriate measures so that the data which is inaccurate or incomplete with regard to the purposes for which it was collected or processed is corrected, deleted or destroyed. The appropriateness of the measures depends in particular on the nature and extent of the data processing and on the risks which the processing entails for the personality and fundamental rights of the data subjects. [6] If the consent of the data subject is required, such consent is only valid if it has been given freely and for one or several specific processing activities and after adequate information. [7] Consent must be given explicitly for: a. the processing of sensitive personal data; b. high risk profiling by a private person; or c. profiling by a federal body.	**Art. 4 Principles** [1] Personal data may only be processed lawfully. [2] Its processing must be carried out in good faith and must be proportionate. [3] Personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law. [4] The collection of personal data and in particular the purpose of its processing must be evident to the data subject. [5] If the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information. Additionally, consent must be given expressly in the case of processing of sensitive personal data or personality profiles	**Art. 5 Principles relating to processing of personal data** (1) Personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to

revised FADP	FADP	GDPR
		safeguard the rights and freedoms of the data subject ('storage limitation'); f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). (2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').
Art. 7 Data protection by design and by default [1] The controller must set up technical and organisational measures in order for the data processing to meet the data protection regulations and in particular the principles set out in Article 6. It considers this obligation from the planning of the processing. [2] The technical and organisational measures must be appropriate in particular with regard to the state of the art, the type and extent of processing, as well as the risks that the processing at hand poses to the personality and the fundamental rights of the data subjects. [3] The controller is additionally bound to ensure through appropriate pre-defined settings that the processing of the personal data is limited to the minimum required by the purpose, unless the data subject directs otherwise.		**Art. 25 Data protection by design and by default** (1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. (2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. (3) (…)
Art. 8 Data security [1] The controller and the processor must ensure, through adequate technical and organisational measures, security of the personal data that appropriately addresses the risk. [2] The measures must enable the avoidance of data security breaches. [3] The Federal Council shall issue provisions on the minimum requirements for data security.	**Art. 7 Data security** [1] Personal data must be protected against unauthorised processing through adequate technical and organisational measures. [2] The Federal Council issues detailed provisions on the minimum standards for data security.	**Art. 32 Security of processing** (1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:; … (2) – (4) (…)
Art. 9 Data processing by processors [1] The processing of personal data may be assigned by agreement or by legislation to a processor if: a. the data is processed only in a manner permitted for the controller itself; and	**Art. 10a Data processing by third parties** [1] The processing of personal data may be assigned to third parties by agreement or by law if: a. the data is processed only in the manner permitted for the instructing party itself; and	**Art. 28 Processor** (1) Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this

revised FADP	FADP	GDPR
b. no statutory or contractual duty of confidentiality prohibits the assignment. [2] The controller must ensure in particular that the processor is able to guarantee data security. [3] The processor may only assign the processing to a third party with the prior authorisation of the controller. [4] It may invoke the same justifications as the controller.	b. it is not prohibited by a statutory or contractual duty of confidentiality. [2] The instructing party must in particular ensure that the third party guarantees data security. [3] Third parties may claim the same justification as the instructing party.	Regulation and ensure the protection of the rights of the data subject. (2) The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. (3) Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: … (4) – (10) (…)
Art. 10 Data protection advisor [1] Private controllers may appoint a data protection advisor. [2] The data protection advisor is the contact point for the data subjects and for the competent data protection authorities responsible for data protection matters in Switzerland. In particular, he or she has the following duties: a. to train and advise the private controller in matters of data protection; b. the participation in the enforcement of data protection regulations. [3] Private controllers may invoke the exception set out in Article 23 paragraph 4 if the following requirements are fulfilled: a. the data protection advisor performs his function towards the controller in a professionally independent manner and without being bound by instructions; b. he does not perform any activities which are incompatible with his tasks as data protection advisor; c. he possesses the necessary professional knowledge; d. the controller publishes the contact details of the data protection advisor and communicates them to the FDPIC. [4] The Federal Council regulates the appointment of data protection advisors by the federal bodies	**Art. 11a Register of data files** [1] – [4] (…) [5] In derogation from the provisions in paragraphs 2 and 3, the controller of data files is not required to declare his files if: a. – d. (…) e. he has designated a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files; f. (…) [6] The Federal Council regulates the modalities for the declaration of data files for registration, the maintenance and the publication of the register, the appointment and duties of the data protection officer under paragraph 5 letter e and the publication of a list of controllers of data files that are relieved of the reporting obligation under paragraph 5 letters e and f.	**Art. 37 Designation of the data protection officer** (1) The controller and the processor shall designate a data protection officer in any case where: a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or c) the core activities of the controller or the processor consist of processing on a large scale of special categories of (2) – (4) (…) (5) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39. (6) The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. (7) The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority **Art. 38 Position of the data protection officer** (1) – (2) (…) (3) The controller and processor shall ensure that the data protection officer does not receive any instructionsregarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data

revised FADP	FADP	GDPR
		protection officer shall directly report to the highest management level of the controller or the processor. (4) – (6) (…) **Art. 39 Tasks of the data protection officer** 1. The data protection officer shall have at least the following tasks: a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; d) to cooperate with the supervisory authority; e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter (2) (…)
Art. 11 Codes of conduct [1] Professional associations, industry associations and business associations whose statutes entitle them to defend the economic interests of their members, as well as federal bodies, may submit codes of conduct to the FDPIC. [2] The FDPIC states his opinion on the codes of conduct and publishes his opinion.		**Art. 40 Codes of conduct** (1) The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises. (2) Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: a) – k) (…) (3) – (4) (5) Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conductor to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisoryauthority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards. (6) – (11) (…)

revised FADP	FADP	GDPR
		Art. 41 Monitoring of approved codes of conduct (1) – (6) (…)
Art. 12 Records of processing activities [1] The controllers and the processors each keep a record of their processing activities. [2] The controller's record contains at least the following information: a. the controller's identity; b. the purpose of the processing; c. a description of the categories of data subjects and the categories of the processed personal data; d. the categories of the recipients; e. if possible the period of storage of the personal data or the criteria to determine the period of storage; f. if possible a general description of the measures to guarantee data security pursuant to Article 8; g. in case of disclosure of data abroad, the name of the state in question and the guarantees according to Article 16 paragraph 2. [3] The processor's record contains information on the identity of the processor and of the controller, the categories of processing activities performed on behalf of the controller as well as the information foreseen in paragraph 2 letters f and g. [4] The federal bodies notify the FDPIC of their records. [5] The Federal Council provides for exceptions for companies that have less than 250 members of staff and whose processing entails only a low risk of infringing the personality of the data subjects	**Art. 11a Register of data files** [1] The Commissioner maintains a register of data files that is accessible online. Anyone may consult the register. [2] Federal bodies must declare all their data files to the Commissioner in order to have them registered. [3] Private persons must declare their data files if: a. they regularly process sensitive personal data or personality profiles; or b. they regularly disclose personal data to third parties. [4] The data files must be declared before they are opened. [5 – 6] (…)	**Art. 30 Records of processing activities** (1) Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; b) the purposes of the processing; c) a description of the categories of data subjects and of the categories of personal data; d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; f) where possible, the envisaged time limits for erasure of the different categories of data; g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). (2) Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: a) –d) (…) (3) The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form. (4) The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request. (5) The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.
Art. 13 Certification [1] The providers of data processing systems or software as well as the controllers and the processors may submit their systems, their products and their services for evaluation by recognised independent certification organisations.	**Art. 11 Certification procedure** [1] In order to improve data protection and data security, the manufacturers of data processing systems or programs as well as private persons or federal bodies that process personal data may submit their systems, procedures and	**Art. 42 Certification** (1) The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating

revised FADP	FADP	GDPR
[2] The Federal Council issues regulations on the recognition of certification procedures and the introduction of a data protection quality label. In doing so, it shall take into account international law and internationally recognised technical norms.	organisation for evaluation by recognised independent certification organisations. [2] The Federal Council shall issue regulations on the recognition of certification procedures and the introduction of a data protection quality label. In doing so, it shall take account of international law and the internationally recognised technical standards.	compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account. (2) – (8) (…) **Art. 43 Certification bodies** (1) – (9) (…)
Section 2: Data processing by private controllers with registered office or residence abroad		
Art. 14 Representative [1] Private controllers with their domicile or residence abroad designate a representative in Switzerland if they process personal data of persons in Switzerland and the data processing fulfils the following requirements: a. The data processing is connected to offering goods or services in Switzerland or to monitoring the behaviour of these persons. b. The processing is extensive. c. It is a regular processing. d. The processing involves a high risk for the personality of the data subjects. [2] The representative serves as a contact point for the data subjects and the FDPIC. [3] The controller publishes the name and address of the representative.		**Art. 27 Representatives of controllers or processors not established in the Union** (1) Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union. (2) The obligation laid down in paragraph 1 of this Article shall not apply to: a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or b) a public authority or body. (3) The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are. (4) The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation. (5) (…)
Art. 15 Duties of the representative [1] The representative shall keep a register of the processing activities of the controller, which contains the information specified in Article 12 paragraph 2. [2] On request, it shall provide the FDPIC with the information contained in the register. [3] On request, it shall provide the data subject with information on how to exercise his rights.		**Art. 30 Records of processing activities** (1) Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: a) – g) (…) (2) – (5) (…)
Section 3 Cross-Border Disclosure of Personal Data		
Art. 16 Principles	**Art. 6 Cross-border disclosure**	**Art. 44 General principle for transfers**

revised FADP	FADP	GDPR
[1] Personal data may be disclosed abroad if the Federal Council has determined that the legislation of the relevant State or international body guarantees an adequate level of protection. [2] In the absence of such a decision by the Federal Council under paragraph 1, personal data may be disclosed abroad only if appropriate protection is guaranteed by: a. an international treaty; b. data protection provisions of a contract between the controller or the processor and its contracting partner, which were communicated beforehand to the FDPIC; c. specific safeguards prepared by the competent federal body and communicated beforehand to the FDPIC; d. standard data protection clauses previously approved, established or recognised by the FDPIC; e. binding corporate rules on data protection which were previously approved by the FDPIC, or by a foreign authority which is responsible for data protection and belongs to a state which guarantees adequate protection. [3] The Federal Council can provide for other adequate safeguards in the sense of paragraph 2.	[1] Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection. [2] In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if: a. sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad; b. the data subject has consented in the specific case; c. the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party; d. disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts; e. disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject; f. the data subject has made the data generally accessible and has not expressly prohibited its processing; g. disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection. [3] The Federal Data Protection and Information Commissioner (the Commissioner, Art. 26) must be informed of the safeguards under paragraph 2 letter a and the data protection rules under paragraph 2 letter g. The Federal Council regulates the details of this duty to provide information.	Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined. **Art. 45 Transfers on the basis of an adequacy decision** (1) A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation. (2) – (9) (…) **Art. 46 Transfers subject to appropriate safeguards** (1) In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. (2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: a) a legally binding and enforceable instrument between public authorities or bodies; b) binding corporate rules in accordance with Article 47; c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

revised FADP	FADP	GDPR
		(3) Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. (4) – (5) (…)
Art. 17 Exceptions [1] By way of derogation from Article 16 paragraphs 1 and 2, personal data may be disclosed abroad if: a. The data subject has explicitly consented to the disclosure; b. The disclosure is directly connected with the conclusion or the performance of a contract: 1. between the controller and the data subject, or 2. between the controller and its contracting partner in the interest of the data subject; c. Disclosure is necessary: 1. in order to safeguard an overriding public interest, or 2. for the establishment, exercise or enforcement of legal claims before a court or another competent foreign authority; d. Disclosure is necessary in order to protect the life or the physical integrity of the data subject or a third party and it is not possible to obtain the consent of the data subject within a reasonable period of time; e. The data subject has made the data generally accessible and has not expressly prohibited its processing; f. The data originates from a register provided for by law which is accessible to the public or to persons with a legitimate interest, provided that the legal conditions for the consultation are met in the specific case. [2] The controller or the processor informs, upon request, the FDPIC of disclosures of personal data under paragraph 1, letters b, nr 2, c and d.		**Art. 49 Derogations for specific situations** (1) In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; d) the transfer is necessary for important reasons of public interest; e) the transfer is necessary for the establishment, exercise or defence of legal claims; f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. … (2) – (6) (…)
Art. 18 Publication of personal data in electronic format If personal data is made generally accessible by means of automated information and communications services for the purpose of providing information to the general public, this is not deemed to be transborder disclosure, even if the data is accessible from abroad.		
Chapter 3: Duties of the controller and the processor		

revised FADP	FADP	GDPR
Art. 19 Duty of information when collecting personal data [1] The controller informs the data subject appropriately about the collection of personal data; such duty of information also applies when data is not collected from the data subject. [2] At the time of collection the controller shall provide to the data subject all information which is required in order for the data subject to assert his rights according to this Act and to ensure transparent processing of data, in particular: a. the controller's identity and contact information; b. the purpose of processing; c. if applicable, the recipients or the categories of recipients to which personal data is disclosed. [3] If data is not collected from the data subject, it additionally informs the data subject of the categories of personal data which is processed. [4] If personal data is disclosed abroad, the controller also informs the data subject of the name of the State or international body and, as the case may be, the safeguards according to Article 16 paragraph 2 or the applicability of one of the exceptions provided for in Article 17. [5] If data is not collected from the data subject, it provides to the data subject the information mentioned in paragraphs 2 to 4 at the latest one month after it received the personal data. If the controller discloses the personal data prior to this date, it informs the data subject at the time of disclosure at the latest.	**Art. 14 Duty to provide information on the collection of sensitive personal data and personality profiles** [1] The controller of the data file is obliged to inform the data subject of the collection of sensitive personal data or personality profiles; this duty to provide information also applies where the data is collected from third parties. [2] The data subject must be notified as a minimum of the following: a. the controller of the data file; b. the purpose of the processing; c. the categories of data recipients if a disclosure of data is planned. [3] If the data is not collected from the data subject, the data subject must be informed at the latest when the data is stored or if the data is not stored, on its first disclosure to a third party. [4] – [5] (…)	**Art. 13 Information to be provided where personal data are collected from the data subject** (1) Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: a) the identity and the contact details of the controller and, where applicable, of the controller's representative; b) the contact details of the data protection officer, where applicable; c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; e) the recipients or categories of recipients of the personal data, if any; f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. (2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; d) the right to lodge a complaint with a supervisory authority; e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; f) (…) (3) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. (4) (…)

revised FADP	FADP	GDPR
		Art. 14 Information to be provided where personal data have not been obtained from the data subject (1) Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: a) – f) (…) (2) (…) (3) The controller shall provide the information referred to in paragraphs 1 and 2: a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed. (4) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. (5) (…)
Art. 20 Exceptions to the duty of information and restrictions [1] The duty of information according to Article 19 ceases to apply if one of the following requirements is met: a. The data subject already has the corresponding information. b. The processing is provided for by law. c. The controller is a private person and is bound by a legal obligation to secrecy. d. The requirements of Article 27 are fulfilled. [2] If personal data is not collected from the data subject, the duty of information shall also not apply if one of the following requirements is met: a. it is not possible to give the information; or b. it requires disproportionate efforts. [3] The controller may restrict, defer or waive the provision of information in the following cases: a. this is required to protect the overriding interests of third parties; b. the information prevents the processing from fulfilling its purpose; c. when the controller is a private person and the following conditions are fulfilled: 1. the measure is required by the controller's overriding interests. 2. the controller does not disclose the personal data to third parties. d. when the controller is a federal body and one of the following requirements is met:	**Art. 14 Duty to provide information on the collection of sensitive personal data and personality profiles** [1] – [3] (…) [4] The duty of the controller of the data file to provide information ceases to apply if the data subject has already been informed or, in cases under paragraph 3, if: a. the storage or the disclosure of the data is expressly provided for by law; or b. the provision of information is not possible or possible only with disproportionate inconvenience or expense. [5] The controller of the data file may refuse, restrict or defer the provision of information subject to the requirements of Article 9 paragraphs 1 and 4.	**Art. 13 Information to be provided where personal data are collected from the data subject** (1) – (3) (…) (4) Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information. **Art. 14 Information to be provided where personal data have not been obtained from the data subject** (1) – (4) (…) (5) Paragraphs 1 to 4 shall not apply where and insofar as: a) the data subject already has the information; b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides

revised FADP	FADP	GDPR
1. a prevailing public interest, in particular the internal or external security of Switzerland, so requires, or 2. the provision of the information is susceptible to compromise an inquiry, investigation or an administrative or judicial proceeding. [4] The condition in paragraph 3 lit. c number 2 is deemed met if the disclosure of personal data takes place between companies controlled by the same legal entity.		appropriate measures to protect the data subject's legitimate interests; or d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.
Art. 21 Duty of information in the case of an automated individual decision [1] The controller informs the data subject of a decision which is taken exclusively on the basis of an automated processing and which has legal effects on the data subject or affects him significantly (automated individual decision). [2] It shall give the data subject upon request the opportunity to state his position. The data subject can request that the decision be reviewed by a natural person. [3] Paragraphs 1 and 2 shall not apply if: a. the decision is directly connected with the conclusion or the performance of a contract between the controller and the data subject and the request of the latter is satisfied, or b. the data subject explicitly consented to the decision being taken in an automated manner. [4] If the automated individual decision comes from a federal body, the latter must designate it as such. Paragraph 2 does not apply if the data subject does not need to be heard before the decision in accordance with Article 30 paragraph 2 of the Administrative Procedure Act of 20 December 1968 (APA) or another federal act.		**Art. 13 Information to be provided where personal data are collected from the data subject** (1) (…) (2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. (3) – (4) (…) **Art. 14 Information to be provided where personal data have not been obtained from the data subject** (1) (…) (2) In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (3) – (5) (…) **Art. 22 Automated individual decision-making, including profiling** (1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. (2) Paragraph 1 shall not apply if the decision: a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or c) is based on the data subject's explicit consent.

revised FADP	FADP	GDPR
		(3) In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. (4) (…)
Art. 22 Data protection impact assessment [1] If the intended data processing may lead to a high risk for the data subject's personality or fundamental rights, the controller must conduct beforehand a data protection impact assessment. If the controller considers performing several similar processing operations, it may establish a joint impact analysis. [2] The existence of a high risk, particularly when new technologies are used, depends on the nature, the extent, the circumstances and the purpose of the processing. Such a risk exists in particular in the following cases: a. processing of sensitive personal data on a broad scale; b. systematic surveillance of extensive public areas. [3] The data protection impact assessment contains a description of the intended processing, an evaluation of the risks as regards the data subject's personality or fundamental rights, as well as the intended measures to protect the data subject's personality or fundamental rights. [4] Private controllers are relieved from their obligation to establish a data protection impact assessment if they are legally bound to perform the processing. [5] The private controller can abstain from establishing a data protection impact assessment if it uses a system, product or service that is certified for the intended use in accordance with Article 13 or if it complies with a code of conduct in accordance with Article 11 which meets the following requirements: a. the code of conduct is based on a data protection impact assessment; b. it provides for measures to protect the personality rights or fundamental rights of the data subject; c. it was submitted to the FDPIC.		**Art. 35 Data protection impact assessment** (1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. (2) (…) (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or c) a systematic monitoring of a publicly accessible area on a large scale. (4) – (6) (…) (7) The assessment shall contain at least: a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. (8) Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment. (9) – (11) (…)

revised FADP	FADP	GDPR
Art. 23 Consultation of the FDPIC [1] The controller consults the FDPIC prior to the processing when the data protection impact assessment shows that the processing presents a high risk for the personality or fundamental rights of the data subject despite the measures envisaged by the controller. [2] The FDPIC informs the controller of his objections against the envisaged processing within two months. This deadline can be extended by one month in cases of complex data processing. [3] If the FDPIC has objections against the envisaged processing, he suggests appropriate measures to the controller. [4] The private controller can abstain from consulting the FDPIC if it consulted the data protection advisor according to Article 10.		**Art. 36 Prior consultation** (1) The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. (2) Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation. (3) – (5) (…)
Art. 24 Notification of data security breaches [1] The controller shall notify the FDPIC as soon as possible of a data security breach that is probable to result in a high risk to the personality rights or the fundamental rights of the data subject. [2] In the notification, it must at least indicate the nature of the data security breach, its consequences and the measures taken or foreseen. [3] The processor shall notify the controller as soon as possible of any data security breach. [4] The controller shall also inform the data subject if this is necessary for the protection of the data subject or if the FDPIC so requests. [5] It can restrict the information to the data subject, defer it or refrain from providing information if: a. there are grounds pursuant to Article 26 paragraph 1, letter b or 2 letter b or a statutory duty of secrecy prohibits it; b. information is impossible or requires disproportionate efforts; or c. the information of the data subject is ensured in an equivalent manner by a public announcement. [6] A notification based on this Article can be used in criminal proceedings against the person subject to notification only with such person's consent		**Art. 33 Notification of a personal data breach to the supervisory authority** (1) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. (2) The processor shall notify the controller without undue delay after becoming aware of a personal data breach. (3) The notification referred to in paragraph 1 shall at least: a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; c) describe the likely consequences of the personal data breach; d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. (4) – (5) (…)

revised FADP	FADP	GDPR
		Art. 34 Communication of a personal data breach to the data subject (1) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. (2) – (4) (…)
Chapter 4: Rights of the Data Subject		
Art. 25 Access right [1] Any person may request information from the controller as to whether personal data concerning him is being processed. [2] The data subject shall receive the information required in order to enable him to assert his rights under this Act and to ensure the transparent processing of data. In any case, the following information is provided to the data subject: a. identity and contact details of the controller; b. the personal data being processed as such; c. the purpose of processing; d. the period of storage of the personal data or, if this is not possible, the criteria used to determine such period; e. the available information on the origin of the personal data, to the extent that it was not collected from the data subject; f. if applicable, the existence of an automated individual decision as well as the logic on which this decision is based; g. if applicable, the recipients or categories of recipients to which the personal data was disclosed as well as the information foreseen in Article 19 paragraph 4. [3] Personal data on the data subject's health may be communicated to the data subject, provided his consent is given, by a healthcare professional designated by him. [4] If the controller has personal data processed by a processor, the controller remains under the obligation to provide information. [5] No one may waive the right to information in advance. [6] The controller provides the requested information free of charge. The Federal Council may provide for exceptions where information shall not be provided free of charge, in particular if the effort involved is disproportionate. [7] As a rule, the information shall be provided within 30 days.	**Art. 8 Right to information** [1] Any person may request information from the controller of a data file as to whether data concerning them is being processed. [2] The controller of a data file must notify the data subject: a. of all available data concerning the subject in the data file, including the available information on the source of the data; b. the purpose of and if applicable the legal basis for the processing as well as the categories of the personal data processed, the other parties involved with the file and the data recipient. [3] The controller of a data file may arrange for data on the health of the data subject to be communicated by a doctor designated by the subject. [4] If the controller of a data file has personal data processed by a third party, the controller remains under an obligation to provide information. The third party is under an obligation to provide information if he does not disclose the identity of the controller or if the controller is not domiciled in Switzerland. [5] The information must normally be provided in writing, in the form of a printout or a photocopy, and is free of charge. The Federal Council regulates exceptions. [6] No one may waive the right to information in advance.	**Art. 15 Right of access by the data subject** (1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: a) the purposes of the processing; b) the categories of personal data concerned; c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; f) the right to lodge a complaint with a supervisory authority; g) where the personal data are not collected from the data subject, any available information as to their source; h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. (2) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer. (3) The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. (4)The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.
Art. 26 Limitations to the Access Right	**Art. 9 Limitation of the duty to provide information**	**Art. 23 Restrictions**

revised FADP	FADP	GDPR
[1] The controller may refuse, restrict or defer provision of information if: a. a formal law provides for it, in particular to protect a professional secret; b. it is required by prevailing interests of third parties; or c. the request for information is manifestly unfounded in particular if it pursues a purpose that is contrary to data protection or is obviously of a frivolous nature. [2] Additionally, it is possible to refuse, restrict or defer the provision of information in the following cases: a. when the controller is a private person and the following conditions are fulfilled: 1. if prevailing interests of the controller require the measure. 2. the controller does not disclose the personal data to a third parties. b. when the controller is a federal body and one of the following requirements is met: 1. the measure is required for a prevailing public interest, in particular the internal or external security of Switzerland, or 2. the provision of information is susceptible to compromise an inquiry, investigation or an administrative or judicial proceeding. [3] The requirement under paragraph 2 lit. a number 2 is considered to be met if the disclosure of personal data takes place between companies controlled by the same legal entity. [4] The controller must indicate the grounds on which it refuses, restricts or defers the provision of the information.	[1] The controller of a data file may refuse, restrict or defer the provision of information where: a. a formal enactment so provides; b. this is required to protect the overriding interests of third parties. [2] A federal body may further refuse, restrict or defer the provision of information where: a. this is required to protect overriding public interests, and in particular the internal or external security of the Confederation; b. the information would jeopardise the outcome of a criminal investigation or any other investigation proceedings. [3] As soon as the reason for refusing, restricting or deferring the provision of information ceases to apply, the federal body must provide the information unless this is impossible or only possible with disproportionate inconvenience or expense. [4] The private controller of a data file may further refuse, restrict or defer the provision of information where his own overriding interests so require and he does not disclose the personal data to third parties. [5] The controller of a data file must indicate the reason why he has refused, restricted or deferred access to information.	(1) Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: a) – j) (…) (2) (…)
Art. 27 Limitations to the access right for media [1] If personal data is used exclusively for publication in the edited section of a periodically published medium, the controller may refuse, restrict or defer provision of information for one of the following reasons: a. the data reveals information about the sources of the information; b. access to draft publications would ensue; c. the publication would jeopardize the free formation of the public opinion. [2] Journalists may also refuse, restrict or defer provision of information if they use the personal data exclusively as their personal work instrument.	**Art. 10 Limitations of the right to information for journalists** [1] The controller of a data file that is used exclusively for publication in the edited section of a periodically published medium may refuse to provide information, limit the information or defer its provision provided: a. the personal data reveals the sources of the information; b. access to the drafts of publications would have to be given; c. the freedom of the public to form its opinion would be prejudiced. [2] Journalists may also refuse restrict or defer information if the data file is being used exclusively as a personal work aid.	**Art. 85 Processing and freedom of expression and information** (1) Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression. (2) – (3) (…)
Art. 28 Right of data portability [1] Any person may request from the controller, free of charge, the disclosure of the personal data that he has disclosed to him in a standard electronic format if: a. the controller processes the data in an automated manner; and b. the data is processed with the consent of the data subject or in direct connection with the conclusion or performance of a contract between the controller and the data subject. [2] In addition, the data subject may request the controller to transfer his personal data to another controller if the requirements in accordance		**Art. 20 Right to data portability** (1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

revised FADP	FADP	GDPR
with paragraph 1 are met and this does not involve a disproportionate effort. [3] The Federal Council may provide for exceptions to this freedom of charge, in particular if the effort involved is disproportionate.		b) the processing is carried out by automated means. (2) In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. (3) The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. (4) The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.
Art. 29 Restrictions on the right to data output and transmission [1] The controller may refuse, restrict or postpone the release and transfer of personal data for the reasons listed in Article 26 paragraphs 1 and 2. [2] The controller must give reasons for refusing, restricting or postponing the release or transfer.		**Art. 23 Restrictions** (1) Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: a) – j) (…) (2) (…)
Chapter 5: Special Provisions for Data Processing by Private Persons		
Art. 30 Violation of the personality [1] Anyone who processes personal data must not unlawfully violate the data subjects' personality. [2] A personality harm exists in particular if: a. personal data is processed in contravention with the principles set forth in Articles 6 and 8; b. personal data is processed against the data subject's express declaration of intent; c. sensitive personal data is disclosed to third parties. [3] In general, there is no violation of the personality if the data subject has made the personal data generally accessible and has not expressly prohibited its processing.	**Art. 12 Breaches of privacy** [1] Anyone who processes personal data must not unlawfully breach the privacy of the data subjects in doing so. [2] In particular, he must not: a. process personal data in contravention of the principles of Articles 4, 5 paragraph 1 and 7 paragraph 1; b. process data pertaining to a person against that person's express wish without justification; c. disclose sensitive personal data or personality profiles to third parties without justification. [3] Normally there is no breach of privacy if the data subject has made the data generally accessible and has not expressly prohibited its processing.	
Art. 31 Justifications [1] A violation of the personality is unlawful unless it is justified by the consent of the data subject, by an overriding private or public interest or by law. [2] An overriding interest of the controller may in particular be considered in the following cases:	**Art. 13 Justification** [1] A breach of privacy is unlawful unless it is justified by the consent of the injured party, by an overriding private or public interest or by law. [2] An overriding interest of the person processing the data shall in particular be considered if that person:	**Art. 6 Lawfulness of processing** (1) Processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

revised FADP	FADP	GDPR
a. The controller processes personal data of the contractual party in direct connection with the conclusion or the performance of a contract. b. The controller is or will be in commercial competition with another person or will be in commercial competition with another person and for this purpose processes personal data that is not disclosed to third parties, except in the case of disclosure that takes place between companies controlled by the same legal entity c. The controller processes personal data in order to verify the data subject's creditworthiness, provided that the following requirements are fulfilled: 1. The processing does neither involve sensitive personal nor high-risk profiling. 2. The data is disclosed to third parties only if the data is required by such third parties for the conclusion or the performance of a contract with the data subject. 3. The data is not older than ten years. 4. The data subject is of age. d. The controller processes the personal data on a professional basis and exclusively for publication in the edited section of a periodically published medium or the data serves the controller exclusively as a personal working instrument, given that no publication takes place. e. The controller processes personal data for purposes not relating to a specific person, in particular for the purposes of research, planning and statistics, provided that the following requirements are fulfilled: 1. The controller shall anonymize the data as soon as the purpose of the processing allows for it or shall take reasonable measures to prevent the identification of the data subjects if anonymization is impossible or requires a disproportionate effort. 2. Sensitive personal data is disclosed to third parties in such a manner that the data subjects may not be identified. If this is not possible, measures must be taken to ensure that third parties only process the data for non-personal related purposes. 3. Results are published in such a manner that the data subjects may not be identified. f. The controller collects personal data on a person of public interest which relates to the public activities of that person.	a. processes personal data in direct connection with the conclusion or the performance of a contract and the personal data is that of a contractual party; b. is or intends to be in commercial competition with another and for this purpose processes personal data without disclosing the data to third parties; c. process data that is neither sensitive personal data nor a personality profile in order to verify the creditworthiness of another, and discloses such data to third parties only if the data is required for the conclusion or the performance of a contract with the data subject; d. processes personal data on a professional basis exclusively for publication in the edited section of a periodically published medium; e. processes personal data for purposes not relating to a specific person, in particular for the purposes of research, planning and statistics and publishes the results in such a manner that the data subjects may not be identified; f. collects data on a person of public interest, provided the data relates to the public activities of that person	b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) processing is necessary for compliance with a legal obligation to which the controller is subject; d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks. (2) – (4) (…) **Art. 9 Processing of special categories of personal data** (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. (2) Paragraph 1 shall not apply if one of the following applies: a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; b) – j) (…) (3) – (4) (…)
Art. 32 Legal claims [1] The data subject may request that incorrect personal data be corrected, unless: a. there is a statutory regulation prohibiting the correction; b. the personal data is being processed for archiving purposes in the public interest. [2] Actions relating to the protection of personality rights are governed by Articles 28, 28a and 28g – 28l of the Civil Code. The claimant may in particular request that: a. a specific data processing be prohibited; b. a specific disclosure of personal data to third parties be prohibited;	**Art. 15 Legal claims** [1] Actions relating to protection of privacy are governed by Articles 28, 28a and 28l of the Civil Code. The plaintiff may in particular request that data processing be stopped, that no data be disclosed to third parties, or that the personal data be corrected or destroyed. [2] Where it is impossible to demonstrate that personal data is accurate or inaccurate, the plaintiff may request that a note to this effect be added to the data. [3] The plaintiff may request that notification of third parties or the publication of the correction, destruction, blocking, and	**Art. 79 Right to an effective judicial remedy against a controller or processor** (1) Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation. (2) (…)

revised FADP	FADP	GDPR
c. personal data be deleted or destroyed. [3] If neither the accuracy nor the inaccuracy of the personal data can be determined, the claimant may request for a note that indicates the objection to be added to the personal data. [4] Furthermore, the claimant may request the correction, the deletion or the destruction, the prohibition of processing or of disclosure to third parties, the note indicating the objection or the judgement be communicated to third parties or published.	in particular the prohibition of disclosure to third parties, the marking of the data as disputed or the court judgment. [4] Actions on the enforcement of a right to information shall be decided by the courts in a simplified procedure under the Civil Procedure Code of 19 December 2008.	**Art. 82 Right to compensation and liability** (1) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. (2) – (6) (…) **Art. 16 Right to rectification** The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. **Art. 17 Right to erasure ('right to be forgotten')** (1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: a) – f) (…) (2) – (3) (…) **Art. 18 Right to restriction of processing** (1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: a) – d) (…) (2) – (3) (…) **Art. 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing** The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it. **Art. 20 Right to data portability** (1) – (4) (…) **Art. 21 Right to object**

revised FADP	FADP	GDPR
		(1) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. (2) – (6) (…)
Chapter 6: Special Provisions for Data Processing by Federal Bodies		(*GDPR basically does not distinguish between regulations for data processing by privates or governmental authorities)*
Art. 33 Control and responsibility in case of joint processing of personal data The Federal Council regulates the control procedures and the responsibility for data protection if the federal body processes personal data together with other federal bodies, with cantonal bodies or with private persons.	**Art. 16 Responsible body and controls** [1] The federal body that processes or arranges for the processing of personal data in fulfilment of its tasks is responsible for data protection. [2] If federal bodies process personal data together with other federal bodies, with cantonal bodies or with private persons, the Federal Council may specifically regulate the control of and responsibility for data protection	
Art. 34 Legal basis [1] Federal bodies may process personal data only if there is a statutory basis for doing so. [2] A statutory basis must figure in a formal law in the following cases: a. The processed data is sensitive personal data. b. It is a matter of profiling. c. The processing purpose or the type and manner of the data processing may result in a serious interference with the fundamental rights of the data subject. [3] For the processing of personal data under paragraph 2 letters a and b, a statutory basis in a substantive law is sufficient if the following requirements are fulfilled: a. The processing is essential for a task defined in a formal law. b. The processing does not involve any special risks affecting the fundamental rights of the data subject. [4] By way of derogation from paragraphs 1 to 3, federal bodies may process personal data if one of the following requirements is fulfilled: a. The Federal Council has authorised processing because it considers the rights of the data subject not to be endangered. b. The data subject has given his consent to the processing in the specific case or made his personal data generally accessible and has not expressly prohibited the processing. c. The processing is required in order to protect the life or the physical integrity of the data subject or a third party and it is not possible to	**Art. 17 Legal basis** [1] Federal bodies may process personal data if there is a statutory basis for doing so. [2] They may process sensitive personal data and personality profiles only if a formal enactment expressly provides therefor or if, by way of exception: a. such processing is essential for a task clearly defined in a formal enactment; b. the Federal Council authorises processing in an individual case because the rights of the data subject are not endangered; or c. the data subject has given his consent in an individual case or made his data general accessible and has not expressly prohibited its processing.	

revised FADP	FADP	GDPR
obtain the consent of the data subject within a reasonable period of time.		
Art. 35 Automated data processing in pilot projects [1] The Federal Council may, before a formal law enters into force, authorise the automated processing of sensitive personal data or other data processing under Article 34 paragraph 2 letters b and c if: a. the tasks based on which the processing is required are regulated in a formal law that has already entered into force; b. adequate measures are taken to limit interferences with the fundamental rights of the data subject to the minimum; and c. for the practical implementation of a data processing a test phase before entry into force is indispensable, in particular for technical reasons. [2] It obtains the FDPIC's opinion in advance. [3] The competent federal body shall provide the Federal Council with an evaluation report at the latest within two years after inception of the pilot project. The report contains a proposal on whether the processing should be continued or terminated. [4] Automated data processing must be terminated in any event if within five years after inception of the pilot project no formal law has entered into force that contains the required legal.	**Art. 17a Automated data processing in pilot projects** [1] The Federal Council may, having consulted the Commissioner and before a formal enactment comes into force, approve the automated processing of sensitive personal data or personality profiles if: a. the tasks that require such processing required are regulated in a formal enactment; b. adequate measures are taken to prevent breaches of privacy; c. a test phase before the formal enactment comes into force is indispensable for the practical implementation of data processing. [2] A test phase may be mandatory for the practical implementation of data processing if:a. the fulfilment of a task requires technical innovations, the effects of which must first be evaluated; b. the fulfilment of a task requires significant organisational or technical measures, the effectiveness of which must first be tested, in particular in the case of cooperation between federal and the cantonal bodies; or c. processing requires that sensitive personal data or personality profiles be transmitted online to cantonal authorities. [3] The Federal Council shall regulate the modalities of automated data processing in an ordinance. [4] The competent federal body shall provide the Federal Council with an evaluation report at the latest within two years of the pilot system coming into operation. The report contains a proposal on whether the processing should be continued or terminated. [5] Automated data processing must be terminated in every case if within five years of the pilot systems coming into operation no formal enactment has come in force that contains the required legal basis.	
Art. 36 Disclosure of personal data [1] Federal bodies may disclose personal data only if a statutory basis in accordance with Article 34 paragraphs 1 to 3 so provides. [2] In derogation from paragraph 1, they may disclose personal data in the specific case if one of the following requirements is fulfilled: a. Disclosure of the data is indispensable to the controller or the recipient for the fulfilment of a statutory task. b. The data subject has consented to the disclosure. c. Disclosure of the data is required in order to protect the life or the physical integrity of the data subject or a third party and it is not	**Art. 19 Disclosure of personal data** [1] Federal bodies may disclose personal data if there is legal basis for doing so in accordance with Article 17 or if: a. the data is indispensable to the recipient in the individual case for the fulfilment of his statutory task; b. the data subject has consented in the individual case; c. the data subject has made the data generally accessible and has not expressly prohibited disclosure; or d. the recipient demonstrates credibly that the data subject is withholding consent or blocking disclosure in order to prevent the enforcement of legal claims or the safeguarding	

revised FADP	FADP	GDPR
possible to obtain the consent of the data subject within a reasonable period of time. d. The data subject has made its data generally accessible and has not expressly prohibited disclosure. e. The recipient credibly demonstrates that the data subject is withholding consent or objects to disclosure in order to prevent the enforcement of legal claims or the safeguarding of other legitimate interests; the data subject must be given the opportunity to comment beforehand, unless this is impossible or involves a disproportionate effort. 3 They may also disclose personal data in the context of official information disclosed to the general public, either ex officio or pursuant to the Freedom of Information Act of 17 December 2004 , if: a. the data pertains to the fulfilment of a public duty; and b. there is an overriding public interest in its disclosure. 4 They may on request also disclose the name, first name, address and date of birth of a person if the requirements of paragraph 1 or 2 are not fulfilled. 5 They may make personal data generally accessible by means of automated information and communication services if a legal basis provides for the publication of such data or if they disclose data on the basis of paragraph 3. If there is no longer a public interest in making such data generally accessible, the data concerned must be deleted from the automated information and communication service. 6 Federal bodies shall refuse or restrict disclosure, or make it subject to conditions, if: a. essential public interests or interests manifestly warranting protection of a data subject so require or b. statutory duties of secrecy or special data protection regulations so require.	of other legitimate interests; the data subject must if possible be given the opportunity to comment beforehand. 1bis Federal bodies may also disclose personal data within the terms of the official information disclosed to the general public, either ex officio or based on the Freedom of Information Act of 17 December 2004 if: a. the personal data concerned is connected with the fulfilment of public duties; and b. there is an overriding public interest in its disclosure. 2 Federal bodies may on request also disclose the name, first name, address and date of birth of a person if the requirements of paragraph1 are not fulfilled. 3 Federal bodies may make personal data accessible online if this is expressly provided for. Sensitive personal data and personality profiles may be made accessible online only if this is expressly provided for in a formal enactment.6 3bis Federal bodies may make personal data generally accessible by means of automated information and communication services if a legal basis is provided for the publication of such data or if they make information accessible to the general public on the basis of paragraph1bis. If there is no longer a public interest in the accessibility of such data, the data concerned must be removed from the automated information and communication service. 4 The federal body shall refuse or restrict disclosure, or make it subject to conditions if: a. essential public interests or clearly legitimate interests of a data subject so require or b. statutory duties of confidentiality or special data protection regulations so require.	
Art. 37 Objection to the disclosure of personal data 1 The data subject that credibly demonstrates an interest warranting protection may object to the disclosure of certain personal data by the competent federal body. 2 The federal body shall refuse such request if one of the following requirements is fulfilled: a. there is a legal duty of disclosure; b. the fulfilment of its task would otherwise be endangered. 3 Article 36 paragraph 3 is reserved.	**Art. 20 Blocking disclosure** 1 A data subject that credibly demonstrates a legitimate interest may request the federal body concerned to block the disclosure of certain personal data. 2 The federal body shall refuse to block disclosure or lift the block if: a. there is a legal duty of disclosure; or b. the fulfilment of its task would otherwise be prejudiced. 3 Any blocking of disclosure is subject to Article 19 paragraph 1bis.	
Art. 38 Offering of documents to the Federal Archive 1 In accordance with the Archiving Act of 26 June 19989, the federal bodies shall offer the Federal Archive all personal data that the federal bodies no longer constantly require.	**Art. 21 Offering documents to the Federal Archives** 1 In accordance with the Archiving Act of 26 June 1998, federal bodies shall offer the Federal Archives all personal data that is no longer in constant use.	

revised FADP	FADP	GDPR
[2] The federal body shall destroy personal data designated by the Federal Archive as not being of archival value unless: a. it is rendered anonymous; b. it must be preserved on evidentiary or security grounds or in order to safeguard the legitimate interests of the data subject.	[2] The federal bodies shall destroy personal data designated by the Federal Archives as not being of archival value unless it: a. is rendered anonymous; b. must be preserved on evidentiary or security grounds or in order to safeguard the legitimate interests of the data subject.	
Art. 39 Data processing for research, planning and statistics [1] Federal bodies may process personal data for purposes not related to specific persons, in particular for research, planning and statistics, if: a. the data is rendered anonymous, as soon as the processing purpose so permits; b. the federal body discloses sensitive personal data to private persons only in such a manner that the data subjects cannot be identified; c. the recipient only passes on the data to third parties with the consent of the federal body which has disclosed the data; and d. the results are only published in such a manner that the data subjects may not be identified. [2] Articles 6 paragraph 3, 34 paragraph 2 and Article 36 paragraph 1 do not apply	**Art. 22 Processing for research, planning and statistics** [1] Federal bodies may process personal data for purposes not related to specific persons, and in particular for research, planning and statistics, if: a. the data is rendered anonymous, as soon as the purpose of the processing permits; b. the recipient only discloses the data with the consent of the federal body and c. the results are published in such a manner that the data subjects may not be identified. [2] The requirements of the following provisions need not be fulfilled: a. Article 4 paragraph 3 on the purpose of processing b. Article17 paragraph 2 on the legal basis for the processing of sensitive personal data and personality profiles; c. Article 19 paragraph 1 on the disclosure of personal data.	
Art. 40 Private law activities of federal bodies If a federal body acts under private law, the provisions for data processing by private persons apply.	**Art. 23 Private law activities of federal bodies** [1] If a federal body acts under private law, the provisions for the processing of personal data by private persons apply. [2] Supervision is governed by the provisions on federal bodies.	
Art. 41 Claims and procedure [1] Anyone with an interest warranting protection may request the responsible federal body to: a. refrain from unlawfully processing the personal data; b. eliminate the consequences of unlawful processing; c. ascertain the unlawfulness of the processing. [2] The claimant may in particular request that the federal body: a. correct, delete or destroy the personal data concerned; b. publish or communicate its decision to third parties, in particular on the correction, deletion or destruction, the objection to disclosure under Article 37 or the note that indicates the objection under paragraph 4. [3] Instead of deleting or destroying the personal data, the federal body restricts the processing if a. the data subject disputes the accuracy of the personal data and if it is not possible to determine the accuracy or the inaccuracy thereof; b. overriding interests of third parties so require; c. an overriding public interest, in particular the internal or external security of Switzerland, so requires;	**Art. 25 Claims and procedure** [1] Anyone with a legitimate interest may request the federal body concerned to: a. refrain from processing personal data unlawfully; b. eliminate the consequences of unlawful processing; c. ascertain whether processing is unlawful. [2] If it is not possible to prove the accuracy or the inaccuracy of personal data, the federal body must mark the data correspondingly. [3] The applicant may in particular request that the federal body: a. corrects or destroys the personal data or blocks its disclosure to third parties; b. communicates its decision to third parties, in particular on the correction, destruction, blocking of the data or marking of the data as disputed, or publishes the decision. 4 The procedure is governed by the Federal Act of 20 December 1968 on Administrative Procedure (Administrative Procedure Act). The exceptions contained in	

revised FADP	FADP	GDPR
d. the deletion or destruction of the data may jeopardise an inquest, an investigation or administrative or judicial proceeding. [4] If it is not possible to determine the accuracy or the inaccuracy of personal data, the federal body attaches to the data a note that indicates the objection. [5] The correction, deletion or destruction of personal data may not be requested with respect to the inventory of publicly accessible libraries, educational institutions, museums, archives or other public memorial institutions. If the applicant can credibly demonstrate an overriding interest, he may request that the institution restrict access to the disputed data. Paragraphs 3 and 4 do not apply. [6] The procedure is governed by the APA10. The exceptions contained in Articles 2 and 3 APA do not apply.	Articles 2 and 3 of the Administrative Procedure Act do not apply.	
Art. 42 Procedure in the event of the disclosure of official documents containing personal data If proceedings relating to access to official documents within the meaning of the Freedom of Information Act of 17 December 2004 that contain personal data are pending, the data subject may in such proceedings claim the rights given to him under Article 41 for those of the documents that are the subject matter of the access proceedings.	**Art. 25[bis] Procedure in the event of the disclosure of official documents containing personal data** For as long as proceedings relating to access to official documents within the meaning of the Freedom of Information Act of 17 December 2004 that contain personal data are ongoing, the data subject may within the terms of such proceedings claim the rights accorded to him on the basis of Article 25 of this Act in relation to those documents that are the subject matter of the access proceedings.	
Chapter 7: Federal Data Protection and Information Commissioner **Section 1: Organisation**		
Art. 43 Appointment and status [1] The head of the FDPIC (the commissioner) is elected by the Federal Assembly. [2] Anyone who is entitled to vote on federal matters is eligible. [3] The employment relationship of the commissioner is governed by the Federal Personnel Act of 24 March 2000 (BPG)12, unless this Act provides otherwise. [4] The commissioner exercises his function independently without asking for or accepting instructions of any authority or third party. He is assigned to the Federal Chancellery for administrative purposes. [5] He has a permanent secretariat and his own budget. He hires his own staff. [6] He is not subject to the system of assessment under Article 4 paragraph 3 BPG.	**Art. 26 Appointment and status** [1] The Commissioner is appointed by the Federal Council for a term of office of four years. The appointment must be approved by the Federal Assembly. [1bis] This term of office shall be extended automatically unless the Federal Council has issued an order no less than six months before its expiry based on materially adequate grounds that the term of office should not be extended. [2] The employment relationship is governed by the Federal Personnel Act of 24 March 2000, unless this Act provides otherwise. [3] The Commissioner shall exercise his duties independently, without receiving directives from any authority. He is assigned to the Federal Chancellery for administrative purposes. [4] He has a permanent secretariat and his own budget. He appoints his own staff.	**Art. 51 Supervisory authority** (1) Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority'). (2) – (4) (…) **Art. 52 Independence** (1) Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation. (2) The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

revised FADP	FADP	GDPR
	[5] The Commissioner is not subject to the system of assessment under Article 4 paragraph 3 of the Federal Personnel Act of 24 March 2000.	(3) (...) (4) Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board. (5) Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned. (6) Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget. **Art. 53 General conditions for the members of the supervisory authority** (1) Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by: - their parliament; - their government; - their head of State; or - an independent body entrusted with the appointment under Member State law. (2) – (4) (…)
Art. 44 Term of office, reappointment and termination of the term of office [1] The term of office of the commissioner is four years and may be renewed twice. It begins on 1 January following the start of the legislative period of the National Council. [2] The commissioner may request the Federal Assembly to be discharged from office at the end of any month subject to six months advance notice. [3] The Federal Assembly may dismiss the commissioner from office before the expiry of his term of office if he: a. wilfully or through gross negligence seriously violates official duties; or b. is permanently unable to fulfil his office.	**Art. 26a Reappointment and termination of the term of office** [1] The Commissioner's term of office may be extended twice. [1bis] This term of office shall be extended automatically unless the Federal Council has issued an order based on materially adequate grounds that the term of office should not be extended. [2] The Commissioner may request the Federal Council to be discharged from office at the end of any month subject to six months advance notice. [3] The Federal Council may dismiss the Commissioner from office before the expiry of his term of office if he: a. wilfully or through gross negligence seriously violates his duties of office; or b. he is permanently unable to fulfil his duties of office.	**Art. 53 (…)** (1) – (2) (…) (3) The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned. (4) A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.
Art. 45 Budget The FDPIC submits the draft of his budget annually to the Federal Council via the Federal Chancellery. The Federal Council forwards it unchanged to the Federal Assembly.		

revised FADP	FADP	GDPR
Art. 46 Incompatibility The commissioner may not be a member of the Federal Assembly or the Federal Council and may not have an employment relationship with the Confederation.		**Art. 52 (…)** (1) – (2) (…) (3) Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not. (4) – (6) (…)
Art. 47 Secondary occupation [1] The commissioner must not carry out any secondary occupation. [2] The Federal Assembly (both chambers together) may permit the commissioner to carry out a secondary employment provided this neither compromises the performance of the function nor independence and standing. The Federal Council's decision in this respect is published	**Art. 26b Secondary occupation** [1] The Commissioner may not carry on another occupation. [2] The Federal Council may permit the Commissioner to carry on another occupation provided this does not compromise his independence and standing. The decision shall be published.	
Art. 48 Self-regulation of the FDPIC By means of appropriate control measures, in particular with respect to data security, the FDPIC shall ensure that the legally compliant enforcement of the federal data protection regulations is guaranteed in his office.		
Section 2: Investigation of breaches of data protection regulations		
Art. 49 Investigation [1] The FDPIC initiates, ex officio or upon notification, an investigation against a federal body or a private person if there are sufficient indications that a data processing could violate the data protection regulations. [2] He may refrain from initiating an investigation if the breach of the data protection regulations is of minor significance. [3] The federal body or the private person will provide the FDPIC with all information and will make available all documents which are necessary for the investigation. The right to refuse to provide information is governed by Articles 16 and 17 APA13 unless Article 50 paragraph 2 provides otherwise. [4] If the data subject notified the FDPIC, he will inform the data subject of the steps undertaken in the matter based on the data subject's notification and the results of the investigation, if any.	**Art. 27 Supervision of federal bodies** [1] (…) [2] The Commissioner investigates cases either on his own initiative or at the request of a third party. [3] In investigating cases, he may request the production of files, obtain information and arrange for processed data to be shown to him. The federal bodies must assist in determining the facts of any case. The right to refuse to testify under Article 16 of the Administrative Procedure Act applies by analogy. [4 – 6] **Art. 29 Investigations and recommendations in the private sector** [1] The Commissioner shall investigate cases in more detail on his own initiative or at the request of a third party if: a. methods of processing are capable of breaching the privacy of larger number of persons (system errors); b. data files must be registered (Art. 11a); c. there is a duty to provide information in terms of Article 6 paragraph 3.	**Art. 57 Tasks** (1) Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: a) monitor and enforce the application of this Regulation; b) – g) (…) h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority; i) – o) (…) (2) (…) (3) The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer. (4) (…)

revised FADP	FADP	GDPR
	[2] To this end, he may request files, obtain information and arrange for processed data to be shown to him. The right to refuse to testify under Article 16 of the Administrative Procedure Act applies by analogy. [3 – 4] (...)	
Art. 50 Powers [1] If the federal body or the private person does not comply with the duty to cooperate, the FDPIC may in the context of the investigation order the following: a. access to all information, documents, registers of the processing activities and personal data which are required for the investigation; b. access to premises and facilities, c. questioning of witnesses; d. evaluations by experts. [2] Professional secrecy is reserved. [3] He may call on other a federal authority or the cantonal or municipal police to enforce the measures in accordance with paragraph 1.		**Art. 58 Powers** (1) Each supervisory authority shall have all of the following investigative powers: a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; b) to carry out investigations in the form of data protection audits; c) to carry out a review on certifications issued pursuant to Article 42(7); d) to notify the controller or the processor of an alleged infringement of this Regulation; e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law. (2) – (6) (…)
Art. 51 Administrative measures [1] If data protection regulations are violated, the FDPIC may order that the processing is fully or partially adjusted, suspended or terminated and that the personal data is fully or partially deleted or destroyed. [2] He may defer or prohibit disclosure abroad if it violates the requirements under Articles 13 or 14 or specific provisions on the disclosure of personal data abroad in other Federal Acts. [3] He may in particular order that the federal body or the private person: a. inform the FDPIC under Articles 16 paragraph 2 letters b and c and 17 paragraph 2; b. take the measures under Articles 7 and 8; c. inform the data subjects under Articles 19 and 21 d. perform a data protection impact assessment under Article 22; e. consult the FDPIC under Article 23; f. inform the FDPIC or, if applicable, the data subjects under Article 24; and g. provide the data subject with the information under Article 25. [4] He may also order that the private controller with its registered office or place of residence abroad designate a representation in accordance with Article 14. [5] If during the investigation the federal body or the private person has taken the necessary measures to restore compliance with the data	**Art. 27 Supervision of federal bodies** [1 – 3] (…) [4] If the investigation reveals that data protection regulations are being breached, the Commissioner shall recommend that the federal body concerned change the method of processing or abandon the processing. He informs the department concerned or the Federal Chancellery of his recommendation. [5] If a recommendation is not complied with or is rejected, he may refer the matter to the department or to the Federal Chancellery for a decision. The decision is communicated to the data subjects in the form of a ruling. [6] The Commissioner has a right of appeal against the ruling under paragraph 5 and against the decision of the appeal authority. **Art. 29 Investigations and recommendations in the private sector** [1 – 2] (…) [3] On the basis of his investigations, the Commissioner may recommend that the method of processing be changed or abandoned.	**Art. 58 Powers** (1) (…) (2) Each supervisory authority shall have all of the following corrective powers: a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; e) to order the controller to communicate a personal data breach to the data subject; f) to impose a temporary or definitive limitation including a ban on processing; g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

revised FADP	FADP	GDPR
protection regulations, the FDPIC may limit himself to issuing a warning.	[4] If a recommendation made by the Commissioner is not complied with or is rejected, he may refer the matter to the Federal Administrative Court for a decision. He has the right to appeal against this decision.	h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; j) to order the suspension of data flows to a recipient in a third country or to an international organisation.
Art. 52 Proceedings [1] Investigation proceedings and decisions under Articles 44 and 45 are governed by the APA. [2] Only the federal body or the private person against whom the investigation was initiated shall be party to the proceedings. [3] The FDPIC may file an appeal against appeal decisions issued by the Federal Administrative Court.	**Art. 33** [1] Legal protection is governed by the general provisions on the administration of federal justice. [2] If the Commissioner establishes in a case investigation under Article 27 paragraph 2 or under Article 29 paragraph 1 that the data subjects are threatened with a disadvantage that cannot be easily remedied, he may apply to the President of the division of the Federal Administrative Court responsible for data protection for interim measures to be taken. The procedure is governed by analogy by Articles 79–84 of the Federal Act of 4 December 1947 on Federal Civil Procedure.	
Art. 53 Coordination [1] Federal administrative authorities which supervise private persons or organisations outside of the Federal Administration in accordance with another federal act invite the FDPIC to submit a statement before they issue a decision pertaining to data protection issues. [2] If the FDPIC has initiated his own investigation against the same party, the two authorities will coordinate their proceedings		
Section 3: Administrative Assistance		
Art. 54 Administrative assistance between Swiss authorities [1] Federal and cantonal authorities provide the FDPIC with the information and personal data required for the performance of his statutory duties. [2] The FDPIC discloses to the following authorities the information and personal data required for the performance of their statutory duties: a. the authorities responsible for data protection in Switzerland; b. the competent criminal prosecution authorities if a criminal offence under Article 65 paragraph 2 is reported; c. the federal authorities as well as the cantonal and municipal police for the enforcement of the measures under Articles 50 paragraph 2 and 51.		**Art. 61 Mutual assistance** (1) Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations. (2) – (9) (…)

revised FADP	FADP	GDPR
Art. 55 Administrative assistance to foreign authorities [1] The FDPIC may exchange information and personal data with foreign authorities responsible for data protection for the performance of their respective statutory duties in the area of data protection if the following requirements are fulfilled: a. The reciprocity of administrative assistance is ensured. b. Information and personal data are only used for the proceedings relating to data protection on which the request for administrative assistance is based. c. The receiving authority undertakes to observe professional, business and manufacturing secrets. d. Information and personal data are only disclosed if the authority which has transmitted them has previously consented to the disclosure. e. The receiving authority undertakes to adhere to the conditions and restrictions of the authority which has transmitted the information and personal data. [2] In order to substantiate his request for administrative assistance or to comply with the request of an authority, the FDPIC may in particular provide the following information: a. the identity of the controller, the processor or other third parties involved; b. the categories of data subjects; c. the identity of data subjects if: 1. the data subjects have consented thereto, or 2. the notification of the identity of the data subjects is indispensable so that the FDPIC or the foreign authority may fulfil their statutory duties; d. processed personal data or categories of processed personal data; e. the purpose of processing; f. recipients or categories of recipients; g. technical and organisational measures. [3] Before the FDPIC discloses information which may contain professional, business or manufacturing secrets to a foreign authority, he informs the natural persons or legal entities concerned who are the holders of these secrets and invites them to comment, unless this is not possible or possible only with disproportionate efforts.		**Art. 50 International cooperation for the protection of personal data** In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to: a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data; b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.
Section 4: Other tasks of the FDPIC		
Art. 56 Register The FDPIC keeps a register on the processing activities of the federal bodies. The register is made public.	**Art. 11a Register of data files** [1] The Commissioner maintains a register of data files that is accessible online. Anyone may consult the register. [2–6] (…)	
Art. 57 Information	**Art. 30 Information**	

revised FADP	FADP	GDPR
[1] The FDPIC reports to the Federal Assembly annually on his activities. He simultaneously submits the report to the Federal Council. The report is published. [2] In cases of general interest, the FDPIC informs the public of his findings and his decisions.	[1] The Commissioner shall submit a report to the Federal Assembly at regular intervals and as required. He shall provide the Federal Council with a copy of the report at the same time. The regular reports are published. [2] In cases of general interest, he informs the general public of his findings and recommendations. He may only publish personal data subject to official secrecy with consent of the authority responsible. If it refuses its consent, the President of the division of the Federal Administrative Court responsible for data protection makes the final decision.	
Art. 58 Additional tasks [1] The FDPIC has in particular the following additional tasks: a. He informs, trains and advises the federal bodies as well as private persons on matters of data protection. b. He supports the cantonal bodies and cooperates with domestic and foreign data protection authorities. c. He raises public awareness, and in particular that of vulnerable private persons, regarding data protection. d. He provides persons at their request with information on how they can exercise their rights. e. He provides an opinion on draft federal legislation and on federal measures which entail a processing of data. f. He carries out the tasks assigned to him under the Freedom of Information Act of 17 December 2004 or other Federal Acts. g. He draws up working tools as a recommendation of good practice for controllers, processors and data subjects; in this respect he considers the particularities of the respective area and the protection of vulnerable private persons. [2] He may also advise federal bodies which are not subject to his supervision according to Articles 2 and 4. The federal bodies may grant him access to their files. [3] The FDPIC is authorised to declare to the foreign authorities responsible for data protection that direct delivery is permitted in Switzerland in the area of data protection, provided Switzerland is granted reciprocity.	**Art. 28 Advice to private persons** The Commissioner advises private persons on data protection matters. **Art. 31 Additional tasks** [1] The Commissioner has the following additional tasks in particular: a. he assists federal and cantonal bodies on data protection issues; b. he provides an opinion on draft federal legislation and on other federal measures that are relevant to data protection; c. he cooperates with domestic and foreign data protection authorities; d. he provides an expert opinion on the extent to which foreign data protection legislation guarantees adequate protection; e. he examines safeguards and data protection rules notified to him under Article 6 paragraph 3; f. he examines the certification procedure under Article11 and may issue recommendations in accordance with Article 27 paragraph 4 or Article 29 paragraph 3;. g. he carries out the tasks assigned to him under the Freedom of Information Act of 17 December 2004; h. he shall raise the level of public awareness of data protection matters. [2] He may also advise bodies of the Federal Administration even if, in accordance with Article 2 paragraph 2 letters c and d, this Act does not apply. The bodies of the Federal Administration may permit him to inspect their files.	
Section 5 Fees		
Art. 59 [1] The FDPIC charges private persons fees for: a. his opinion on a code of conduct under Article 11 paragraph 2;		**Art. 57 Tasks** (1) – (2) (…) (3) The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer

revised FADP	FADP	GDPR
b. his approval of standard data protection clauses and binding corporate rules on data protection under Article 16 paragraph 2 letters d and e; c. his consultation based on a data protection impact assessment under Article 23 paragraph 2; d. preliminary injunctions and measures taken under Article 51; and e. providing his advice on matters of data protection under Article 58 paragraph 1 letter a. [2] The Federal Council determines the amount of fees. [3] It may determine in which cases it is possible to refrain from charging a fee or to reduce it.		(4) (…)
Chapter 8: Criminal Provisions		
Art. 60 Breach of obligations to provide access and information or to cooperate [1] On complaint, private persons are liable to a fine of up to 250,000 Swiss Francs if they: a. breach their obligations under Articles 19, 21 and 25–27 by wilfully providing false or incomplete information; b. wilfully fail: 1. to inform the data subject pursuant to Articles 19 paragraph 1 and 21 paragraph 1; or 2. to provide the data subject with the information required under Article 19 paragraph 2. [2] Private persons are liable to a fine of up to 250,000 Swiss Francs if, in violation of Article 49 paragraph 3, they wilfully provide false information to the FDPIC in the context of an investigation or wilfully refuse to cooperate.	**Art. 34 Breach of obligations to provide information, to register or to cooperate** [1] On complaint, private persons are liable to a fine if they: a. breach their obligations under Articles 8–10 and 14, in that they wilfully provide false or incomplete information; or b. wilfully fail: 1. to inform the data subject in accordance with Article 14 paragraph 1, or 2. to provide information required under Article 14 paragraph 2. [2] Private persons are liable to a fine3 if they wilfully: a. fail to provide information in accordance with Article 6 paragraph 3 or to declare files in accordance with Article11a or who in doing so wilfully provide false information; or b. provide the Commissioner with false information in the course of a case investigation (Art. 29) or who refuse to cooperate.	**Art. 83 General conditions for imposing administrative fines** (1) Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive. (2) – (3) (…) (4) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; b) – c) (…) (5) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; b) the data subjects' rights pursuant to Articles 12 to 22; c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; d) any obligations pursuant to Member State law adopted under Chapter IX; e) (6) – (9) (…)
Art. 61 Violation of duties of diligence On complaint, private persons are liable to a fine of up to 250,000 Swiss Francs if they wilfully:		

revised FADP	FADP	GDPR
a. disclose personal data abroad in violation of Article 16 paragraphs 1 and 2 and without the conditions set forth in Article 17 being met; b. assign the data processing to a processor without the conditions set forth in Article 9 paragraphs 1 and 2 being met; c. fail to comply with the minimum data security requirements which the Federal Council has issued under Article 8 paragraph 3.		
Art. 62 Breach of professional confidentiality [1] If a person wilfully discloses secret personal data of which he has gained knowledge while exercising his profession which requires knowledge of such data, he shall be liable on complaint to a fine of up to 250, 000 Swiss Francs. [2] The same penalty applies to anyone who wilfully discloses secret personal data of which he has gained knowledge in the course of his activities for a person bound by a confidentiality obligation or in the course of training with such a person. [3] The disclosure of secret personal data remains punishable after termination of such professional activities or training.	**Art. 35 Breach of professional confidentiality** [1] Anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to their knowledge in the course of their professional activities where such activities require the knowledge of such data is, on complaint, liable to a fine. [2] The same penalties apply to anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to their knowledge in the course of their activities for a person bound by professional confidentiality or in the course of training with such a person. [3] The unauthorised disclosure of confidential, sensitive personal data or personality profiles remains an offence after termination of such professional activities or training.	
Art. 63 Disregard of decisions Private persons shall be liable to a fine of up to 250,000 Swiss Francs if they wilfully fail to comply with a decision issued by the FDPIC with reference to the criminal penalty of this Article or a decision issued by the appellate authorities.		**Art. 83 General conditions for imposing administrative fines** (1) – (3) (…) (5) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: a) – d) (…) e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). (6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. (7) – (9) (…)
Art. 64 Violations committed within undertakings [1] For violations committed within undertakings, Articles 6 and 7 of the Federal Act of 22 March 1974 on Administrative Criminal Law shall apply. [2] If a fine not exceeding 50,000 Swiss Francs could come into consideration and Administrative Criminal Law required investigative measures that would be disproportionate in comparison with the		

revised FADP	FADP	GDPR
penalty incurred, the authority may abstain from prosecuting these persons and instead sentence the undertaking to the payment of the fine (Article 7 of the Administrative Criminal Law).		
Art. 65 Jurisdiction [1] The cantons are responsible for the prosecution and the judgment of criminal acts. [2] The FDPIC may report a criminal offence to the competent criminal prosecution authorities and exercise the rights of a private plaintiff in the proceedings.		**Art. 55 Zuständigkeit** (1) Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State. (2) Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply. (3) (…) **Art. 56 Competence of the lead supervisory authority** (1) Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60. (2) By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State. (3) – (6) (…)
Art. 66 Statute of limitations for criminal prosecution The right to criminally prosecute is subject to a statute of limitations of five years.		
Chapter 9: Conclusion of International Treaties		
Art. 67 The Federal Council may conclude international treaties concerning:. a. the international cooperation between data protection authorities; b. the mutual recognition of an adequate level of protection for the disclosure of personal data abroad.	**Art. 36 Implementation** [1] The Federal Council shall issue the implementing provisions. [2] [3] It may provide for derogations from Articles 8 and 9 in relation to the provision of information by Swiss diplomatic and consular representations abroad. [4] It may also specify: a. which data files require processing regulations; b. the requirements under which a federal body may arrange for the processing of personal data by a third party or for a third party; c. how the means of identification of persons may be used.	

revised FADP	FADP	GDPR
	[5] It may conclude international treaties on data protection provided they comply with the principles of this Act. [6] It regulates how data files must be secured where the data may constitute a danger to life and limb for the data subjects in the event of war or other crisis.	
Chapter 10: Final provisions		
Art. 68 Repeal and amendments of other legislation The repeal and the amendments of other legislation are set forth in annex 1.		
Art. 69 Transitional provisions concerning ongoing processing Articles 7, 22 and 23 do not apply to data processing operations that were started before the entry into force of this law, if the purpose of the processing remains unchanged and no new data is obtained		
Art. 70 Transitional provisions concerning ongoing proceedings This Act does not apply to investigations of the FDPIC which are pending at the time of its entry into force, nor to pending appeals against first instance decisions rendered before its entry into force. In these matters, the previous law applies.		
Art. 71 Transitional provision concerning data pertaining to legal entities For federal bodies, the provisions of other federal regulations that concern personal data continue to apply to data pertaining to legal entities for three years after the entry into force of this Act. During that time, the federal bodies may in particular continue to disclose the data pertaining to legal entities under Article 57s, paragraph 1 and 2, of the Act of 21 March 1997 on the Organisation of the Government and the Administration, if the federal bodies are entitled to disclose personal based on a legal basis.		
Art. 72 Transitional provision concerning the election and termination of the term of office of the commissioner The election of the commissioner and the termination of his term of office shall be governed by the law in force until the end of the legislative period in which this Act enters into force.		
Art. 73 Coordination Coordination with other acts is set out in annex 2.		
Art. 74 Referendum and entry into force [1] This Act is subject to an optional referendum. [2] The Federal Council determines the date of entry into force.		