swissstaffing

Factsheet: Revised Federal Act on Data Protection (revFADP)

Implications for recruitment service providers in Switzerland

1. Initial Situation

The completely revised version of the Federal Act on Data Protection (revFADP) will come into force on September 1, 2023 along with the new Data Protection Ordinance (DPO) and the new Ordinance on Data Protection Certification (DPCO). There will be no transition period.

When the revFADP comes into effect, recruitment service providers will have to comply with new obligations and will need to have taken the necessary steps to do so. Therefore, this document will describe these obligations in detail. Any references to the relevant legal provisions are referring to provisions in the revised Federal Act on Data Protection (revFADP).

The revFADP aims to protect the personality rights and fundamental rights of individuals whose personal data (hereinafter also referred to as "Data") is processed (Article 1 revFADP). It applies to the processing of the personal data of natural persons by private companies and federal agencies (Article 2 (1) revFADP).

The revFADP has several objectives:

- To eliminate the deficiencies of the existing FADP from 1992, which have arisen as a result of rapid technological advances.
- To keep abreast of developments in the European Union and ensure data protection in Switzerland is harmonized with the EU General Data Protection Regulation (EU GDPR). This has been in effect since May 25, 2018 (see swissstaffing Fact Sheet from May 2018). [For further information on adjustments to be made by companies that have already implemented the requirements of the EU GDPR, see the annex titled CHECKLIST 1: ADAPTING FROM THE EU GDPR TO THE REVFADP]
- To promote good practices by increasing the responsibilities and duties of data controllers and the rights of people whose data is processed, as well as the supervisory authority of the Federal Data Protection and Information Commissioner (FDPIC).

2. What is staying the same when the revFADP comes into force?

The fundamental principles of data processing will remain unchanged under the revFADP. As a result, it will continue to be the case that, if the following principles of data processing are complied with, no consent or justification is required in principle before data can be processed (Article 6, 7 and 8 in conjunction with Article 30 revFADP).

- Data may only be collected in accordance with the law. This means that it cannot be obtained through threats, deception or without the knowledge of the data subject (Article 6 (1) revFADP).
- Data processing must be carried out in good faith. This means that honesty, trustworthiness and considerate conduct are imperative (Article 6 (2) revFADP).
- The principle of proportionality must be observed. This means that, in each individual case, the minimum amount of data necessary for processing should be processed (Article 6 (2) and (4) revFADP).
- The data subject must be made aware that personal data is being procured and, in particular, the purpose of the processing; the purpose must either be stated at the time of procurement or be evident from the

circumstances (Article 6 (3) revFADP).

- Anyone who processes personal data must ensure that it is correct (Article 6 (5) revFADP).
- Data security must be ensured; this means that personal data must be protected from unauthorized processing through appropriate technical and organizational measures (Article 8 revFADP).

As in the previous FADP, personality rights are deemed to have been infringed if personal data is processed even though one of the general principles listed above is violated or if the data subject has expressly prohibited the processing of their data (Article 30 (1) and (2) revFADP). However, personal data may still be processed in these cases if there is a legal justification for doing so. Legal justifications may include the consent of the data subject, an overriding private or public interest, or legislation (Article 31 (1) revFADP). Article 31 (2) revFADP lists cases in which the person processing the data (a controller within the meaning of the revFADP) may be considered to have an overriding private interest in the data processing.

Alongside the general provisions in the revFADP, the processing of personal data for employers in Switzerland is also governed, as before, in Article 328b of the Swiss Code of Obligations (OR) and for recruitment agencies and staff leasing agencies in the Employment Services Act (AVG) and the Employment Services Ordinance (AVV). These provisions primarily put in concrete terms the principle of proportionality under data protection law (Article 6 (2) revFADP). This means that any clauses that were developed in the context of the EU GDPR may be referred to with regard to processing personal data in a personnel context [see also EXAMPLE 1: SAMPLE CONSENT CLAUSE and EXAMPLE 2: SAMPLE DATA PROTECTION AND CONSENT CLAUSE IN GENERAL TERMS AND CONDITIONS in the annex to this Factsheet for sample clauses that have been updated to conform to revFADP]. Particular attention should be paid to the following points:

- The recruitment agency or staff leasing agency may only collect personal data if it is required to provide the recruitment or staff leasing service, and only for the duration that it is required (Article 7 (3) and Article 18 (3) AVG). If the staffing service provider obtains references about candidates, this requires the consent of the data subject (Article 47 (1)(b) and Article 19 (1)(b) AVV).
- The processing of a candidate's application is justified by an overriding private interest on the part of the recruitment or staff leasing agency in processing personal data in order to review the application and pass it on to the relevant employer or contracting company. Because this data has been collected for a particular purpose, the collection of any additional data or the storage and subsequent use of applicant data after the employment process is complete require the consent of the applicant.
- After the application process is complete, applicant data must be deleted. Only the contract may still be retained for the purposes of invoicing, for which there is a statutory retention period of 10 years. Beyond this, any storage of data – in other words the failure to delete personal information or the transmission of this information to other potential employers – requires the consent of the applicant.

In certain cases, it may be necessary to collect particularly sensitive personal data (e.g. health information) as part of the recruitment or staff leasing process (see also Clause 3.3 of this Factsheet). If particularly sensitive personal data are shared by the applicant in their application materials, these may only be processed within the context of the application. If this data is used for other purposes, thus requiring the consent of the applicant, this must be expressly obtained.

swissstaffing

3. What reforms will the revFADP bring?

3.1 No longer any protections for legal entities

The revFADP now only protects the data of natural persons and no longer covers the data of legal entities such as that of a stock corporation or associations (cf. Article 2 revFADP). These are protected by company law and by the protection of personality rights under the Civil Code.

3.2 New terms: Data controller and data processor

Instead of talking about the owner of a data collection, as was previously the case, the revised document refers to the new terms data controller and data processor. Data controllers are private companies (legal entities) that decide the purpose and methods of the processing of personal data, either alone or in collaboration with others (Article 5 (j) revFADP). In the case of staff leasing, the staff leasing agency is the data controller together with the future contracting company, if applicable. As the legal employer, the staff leasing agency is the employee's first point of contact and processes personal data for the application process. If a suitable contracting company is found, the personal data is transmitted to this company, meaning that the contracting company and the staff leasing agency are processing some of the data simultaneously and are therefore both considered data controllers under the revFADP.

On the other hand, in the case of permanent recruitment, when the candidate has been successfully placed, the employer processes the personal data for its own purposes in the future, making it the sole data controller from that point on.

Data processors are private individuals who are usually also legal entities, who process personal data on behalf of the controller (Article 5 (j) revFADP). Some examples could include IT service providers to whom the staffing service provider outsources data processing via cloud technology, or service providers that handle the payroll for the staffing service provider's employees.

3.3 Expansion of the range of particularly sensitive personal data

Particularly sensitive personal data (including health records and political information) have been expanded to include biometric and genetic data (Article 5 (c) revFADP). To process particularly sensitive personal data, stricter requirements must be met than for processing "normal" personal data. If processing requires the consent of the data subject, this must be expressly obtained (Article 6 (7)(a) revFADP).

3.4 Profiling and high-risk profiling

Technological developments now allow us to automate the collection, processing, combination and analysis of vast quantities of data on an increasingly large scale in order to identify trends, correlations and other characteristics, which can then be attributed to particular groups. These comparison groups allow the characteristics or behavior of individual natural persons to be determined or predicted, which is why the term "profiling" has been introduced in the revFADP. A distinction is made between "normal" profiling and high-risk profiling. Normal profiling is any kind of automated processing of personal data that involves using this data to assess particular personal aspects that relate to a natural person, particularly to analyze or predict aspects relating to the work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or change of location of that natural person (Article 5 (f) revFADP). This kind of normal profiling occurs, for example, when a seller writes to all buyers of certain wines because the seller believes they are most likely to be interested in making a new purchase of these wines. The revFADP does not restrict this behavior any more or less than any other data processing.

If profiling causes data to be linked, allowing essential aspects of the personality of a natural person to be assessed, that is high-risk profiling. Processing of this nature involves a high risk to the personality rights or fundamental rights of the data subject. Some practical examples here would be a credit check or fraud analyses. In the future, these types of processing will probably increasingly play a role in application processes. High-risk profiling is subject to stricter requirements when it comes to the processing of personal data. Insofar as the consent of the data subject is required, this must be expressly obtained (Article 6 (7)(b) revFADP). Usually, a data protection impact assessment (DPIA) must be carried out (cf. Clause 3.11).

3.5 Data protection by design and data protection by default

In accordance with the new principle of data protection by design introduced in the revFADP, the data controller is obligated to plan the technical and organizational aspects of data processing in such a way that it complies with data protection legislation (Article 7 (1) and (2) revFADP). In other words, software and hardware must be designed and developed from the earliest stages with adherence to the principles of data processing in mind (cf. Clause 2 above). Moreover, the data controller must ensure, in accordance with the principle of data protection by default, that the default settings are such that the processing of personal data is limited to the minimum necessary for the purpose of use, unless the data subject specifies otherwise (Article 7 (3) revFADP).

3.6 Comprehensive right to be informed

According to the revFADP, the data subject has a comprehensive right to information about the processing of their personal data (Article 19 et seq. revFADP). Privacy notices on websites, apps, and forms are examples of places that expressly state how personal data is processed specifically and how the information can be provided to data subjects. The following information must be provided to data subjects as a minimum:

- the identity and contact details of the data controller;
- the purpose of the data processing;
- the categories of personal data being processed (if the data is not obtained directly from the person);
- if applicable, the recipient or categories of recipients to whom the personal data is provided; and
- the countries to which the personal data is transmitted and the legal basis on which this takes place (any contractual guarantees or exemptions invoked) [cf. Clause 3.9 and the annex titled CHECKLIST 2: IMPLEMENTING THE REQUIREMENTS OF THE REVFADP].

3.7 Expansion of the rights of data subjects

The revFADP continues to grant the data subject rights of access, erasure and blocking (restriction) of their personal data and amends these rights in some cases. Data subjects are entitled to all the information needed to exercise their rights and ensure data processing is carried out in a transparent manner (Article 25 (2) revFADP). Access to the information is free of charge on principle and must usually be provided within 30 days (Article 25 (6) and (7) revFADP). The revFADP also introduces the right to data portability (Article 28 et seq. revFADP). This means that a person can request that the data controller hand over personal data that concerns them and that was previously disclosed to them, as well as personal data processed automatically on the basis of consent or a contract, in a commonly used electronic format, or that the controller transfer this data to another data controller (Article 28 revFADP).

3.8 Right to veto the processing of personal data by data processors

According to the revFADP, the processing of personal data may be transferred to third parties by agreement or by law if the data is processed in the same way as the staffing service provider itself would be permitted to do and if there are no legal or contractual confidentiality obligations that prohibit outsourcing (Article 9 (1) revFADP). Some examples of the transfer of data processing to third parties (contractors) could be data processing for the purposes of payroll, administrative accounting through datacenters, outsourcing data processing to an IT service provider via cloud technology, or the use of a third-party service provider to send out newsletters. In these cases, the data controller remains responsible for the data processing. This means the controller must ensure that any contracted third parties can guarantee data security (Article 8 (2) revFADP). Now, the data processor may only transfer the processing to a third party with the prior approval of the controller company (known as the right to veto) (Article 9 (3) revFADP). The data processor must inform the controller of any data security breaches as quickly as possible (Article 24 (3) revFADP). It is advisable to include an obligation to comply with data protection requirements in the relevant contract with the service provider or in the General Terms and Conditions. An example of a clause like this in General Terms and Conditions can be found in the annex [EXAMPLE 3: SAMPLE COMMISSIONED DATA PROCESSING CLAUSE IN GENERAL TERMS AND CONDITIONS].

3.9 List of countries with equivalent data protection published by the Swiss Federal Council

According to the revFADP, when data is disclosed abroad – for example, when using a service provider that is based abroad (e.g. an IT service provider based in the USA) – steps must be taken to ensure the personality rights of the data subjects are not jeopardized. Data may be transferred to countries with equivalent levels of data protection, including outsourcing to contractors based abroad, without any further action (Article 16 (1) revFADP). A list of countries with equivalent data protection will be published. It includes Switzerland and all EU countries. The list of countries with equivalent data protection is now published by the Swiss Federal Council and no longer by the Federal Data Protection and Information Commissioner (FDPIC).

If there is no legislation that guarantees an adequate degree of data protection, personal data may only be disclosed abroad if there are sufficient measures in place to guarantee protection (Article 16 (2) revFADP). More specifically, these sufficient measures to guarantee protection include the EU's Standard Contractual Clauses (SCC). There are some possible exceptions to this, including if the data subject has expressly consented to the data being disclosed (Article 17 (1)(a) revFADP).

3.10 Obligation to report data security breaches

In the event of a data security breach, the company acting as the data controller must inform the FDPIC (and the data subjects, if applicable) as soon as possible of any breaches of data security that are likely to incur a high risk for the data subject (Article 24 (1) revFADP). This includes, for example, the theft of personal data by internal or external persons (e.g. hackers) or the destruction of information, for example due to user errors, technical errors, viruses or hacker attacks. As a rule, this report should be made by management. However, it is the members of the board of directors who are ultimately responsible for this as part of their risk management (cf. Article 754 (1) OR). The company acting as data controller must document any breaches. The documentation must contain all the facts relevant to the incidents, as well as the consequences and measures taken. It should be retained for a minimum of two years after the report is made (Article 15 (4) DPO).

3.11 New formal obligations under revFADP

Finally, staffing service providers will have to comply with formal obligations in the future that relate to the processing of personal data:

- Nominating a central unit for data protection (e.g. legal service, IT).
- A company with more than 250 employees must keep a register of all personal data processing activities carried out (Article 12 revFADP). Temporary employees are included in the 250 figure. In some exceptional cases, companies with fewer than 250 employees must also keep a register, specifically if they are processing particularly sensitive personal data on a large scale or carrying out high-risk profiling.

  The register kept by the data controller must contain the following information as a minimum:
  - Identity of the controller,
  - Purpose of processing,
  - Description of the categories of data subject and the categories of personal data being processed,
  - Categories of recipients,
  - Retention period of personal data or the criteria for determining the retention period,
  - Description of data security measures and
  - in the event of data disclosure abroad, name of the country and the guarantee ensuring adequate data protection.
- The staffing service provider acting as a data controller in the meaning of revFADP must implement technical and organizational information security measures in order to adequately protect personal data (Article 8 revFADP) (see also the link to the FDPIC's guidelines on the technical and organizational measures relating to the current FADP in the annex: USEFUL LINKS).
- The company acting as data controller must compile a data protection impact assessment (DPIA) beforehand if their data processing may involve a high risk to the personality rights or fundamental rights of the data subjects. Therefore, if a company plans to carry out more sensitive undertakings such as introducing special applications, it has an obligation to conduct and document a formalized risk analysis. Various circumstances, including the use of new technologies as well as the type, scope, circumstances and purpose of processing personal data, are used to determine whether a high risk is present. The DPIA itself contains a description of the proposed processing, an evaluation of the risks to the personality rights or fundamental rights of the data subject, and the measures taken in relation to this to protect the data subject's personality rights and fundamental rights. It is also, in essence, a risk analysis (Article 22 (f) revFADP). Some cantons, including the Canton of Zurich, have published forms to help prepare a DPIA [see annex: USEFUL LINKS].
- Finally, employees also need to be informed and trained on data protection.

4. Sanctions

The fines for violating these rules have also significantly increased in the revFADP. Anyone who intentionally violates the following obligations of the revFADP (including any intentional acceptance of the sanctioned conduct) must expect a fine of up to 250,000 Swiss francs (Article 60 et seq. revFADP):

- false or incomplete information;
- violation of the data subject's right to be informed;
- non-compliance with the minimum data security requirements;

- unauthorized disclosure of data abroad;
- commissioned data processing that does not comply with the legal requirements;
- breach of confidentiality requirements.

Moreover, in the revFADP, responsible individuals within companies including CEOs, CFOs and CIOs can be sanctioned directly. Though most of these sanctions are offenses that are prosecuted only if a data subject brings a case.

swissstaffing

5. Action required by Swiss staffing service providers

No. 1 **Review of internet presence** (Privacy statement, General Terms and Conditions (AGB), applications, newsletter delivery, declarations of consent)	**No. 2** **Review / conclusion of contracts in the case of data processing by third parties (incl. transfer of data abroad)** (Contract, decisional authority, no breach of confidentiality obligations, data security, right to veto, obligation to report in the case of data transfer, reasonable guarantees if required)
No. 3 **Review whether data protection principles are being observed** (Legitimacy, good faith, proportionality, intended purpose, data integrity, data security)	**No. 4** **Development of process for reporting any data security breaches** (reporting to FDPIC/data subject if high risk)
No. 5 **Development of processes concerning rights of data subjects** (Access process, rectification process, erasure process, objection process, process for data portability)	**No. 6** **Compliance with formal obligations** (Central data protection unit, training of employees, register of processing activities if over 250 employees, DPIA)

For a list of concrete actions to be taken by staffing service providers, see also the annex titled CHECKLIST 2: IMPLEMENTING THE REQUIREMENTS OF THE REVFADP.

If you have any queries, please do not hesitate to contact the swissstaffing legal service on +41 (0)44 / 388 95 75 or at legal@swissstaffing.ch.

Zurich, March 2023

swissstaffing

CHECKLIST 1: ADAPTING FROM THE EU GDPR TO THE REVFADP

If you have already implemented the requirements of the EU GDPR, this checklist allows you to verify what adjustments you still need to make in light of the revFADP.

Important: It is quite possible that the EU GDPR will also be applied in addition to the revFADP, so the requirements may apply in parallel.

<table>
<tr>
<td>No. 1</td>
<td>Applicability of the revFADP

Often, the compiled documents only refer to the EU GDPR. They must now be extended to include reference to the revFADP.</td>
<td>Documents refer to how the revFADP is applied alongside the EU GDPR.</td>
<td>☐</td>
</tr>
<tr>
<td>No. 2</td>
<td>Terminology

The German terminology used in the revFADP is slightly different to the terms used in the EU GDPR:

<table>
<tr><th>revFADP</th><th>EU GDPR</th></tr>
<tr><td>Bearbeitung (processing)</td><td>Verarbeitung (processing)</td></tr>
<tr><td>Personendaten (personal data)</td><td>personenbezogene Daten (personal data)</td></tr>
<tr><td>besonders schützenswerte Personendaten (particularly sensitive personal data)</td><td>besonderer Kategorien personenbezogener Daten (special categories of personal data)</td></tr>
<tr><td>Datensicherheitsverletzung (data security breach)</td><td>Datenschutzverletzung (personal data breach)</td></tr>
</table>
</td>
<td>The following German terms have been adapted in the documentation: Verarbeitung/Bearbeitung (processing), personenbezogene Daten/Personendaten (personal data), besondere Kategorien von Daten/besonders schützenswerte Daten (special categories of personal data/particularly sensitive personal data), Datenschutzverletzung/Datensicherheitsverletzung (personal data breach/data security breach)</td>
<td>☐</td>
</tr>
<tr>
<td>No. 3</td>
<td>Expanded definition of particularly sensitive personal data

Data on administrative and criminal prosecutions or sanctions and data on social assistance measures are considered to be particularly sensitive personal data under the revFADP. This means that, if consent is required, it must be expressly obtained.</td>
<td>If consent is required for the processing of data regarding administrative and criminal proceedings or sanctions or data on social assistance measures, this consent is</td>
<td>☐</td>
</tr>
</table>

		expressly obtained.	
No. 4	**Fulfillment of obligations relating to the right to be informed** The obligations that apply in Switzerland relating to data subjects' right to be informed are slightly different to those under the EU GDPR. Privacy notices must include information about the destination country if data is transferred abroad.	The privacy notice has been updated to include information about the destination country if data is transferred abroad.	☐
No. 5	**Register of processing activities** The register of processing activities under revFADP must state the destination country of any data that is transferred abroad.	The register of processing activities has been updated to include information on the destination country of any data transferred abroad.	☐
No. 6	**Process in the event of a data security breach** Under the EU GDPR, personal data breaches that incur a risk to the data subjects must be reported within 72 hours (data theft or misuse of data). Under the revFADP, any breach of data security must be reported to the Federal Data Protection and Information Commissioner (FDPIC) as quickly as possible if it incurs a high risk to the data subjects. The risk threshold at which a breach must be reported to the data protection authority and/or the data subjects is defined differently in the revFADP than in the EU GDPR.	The deadline for reporting has been adapted from "within 72 hours" to "as quickly as possible", and the risk threshold has been adjusted.	☐
No. 7	**Process in the event of a request by the data subject** In contrast to the EU GDPR, the revFADP contains a general provision allowing data subjects to be provided with the necessary information required to assert their rights and to ensure data processing is transparent. This is in addition to the minimum information that must be provided in every case to a data subject who requests information.	The process for requests by data subjects has been updated to allow data subjects to obtain any and all information required to assert their rights and ensure data processing is transparent.	☐

No. 8	**Mandatory recordkeeping** In contrast to the EU GDPR, the revFADP does not recognize the general principle of “accountability”. However, it does contain more extensive data security obligations than the EU GDPR when it comes to processing particularly sensitive data on a large scale and carrying out high-risk profiling, if the preventive measures do not ensure data protection. In line with this, mandatory recordkeeping obligations apply when it comes to storing, modifying, reading, disclosing, erasing and destroying personal data, and processing regulations must be drawn up with information about the internal organization, data processing and control processes, and measures to ensure data security. (Article 4 (1) of the new DPO). This means that records must also be kept in particular if it could not otherwise be subsequently determined whether the data was processed for the purpose for which it was collected or disclosed.	Insofar as automated processing of particularly sensitive data is being carried out on a large scale or high-risk profiling is taking place and the preventive measures do not ensure data security, mandatory recordkeeping obligations are observed.	☐

swissstaffing

CHECKLIST 2: IMPLEMENTING THE REQUIREMENTS OF THE REVFADP

This checklist will enable you to implement the requirements of the revFADP and review your status quo.

No. 1	**Review internet presence** Your website is the face you put forward to the world. It is freely and publicly accessible. Your privacy notice informs users on how personal data is processed and thus fulfills the requirements that arise from the right to be informed under the revFADP.	The privacy notice is correct, complete and up to date.	☐
		The privacy notice is placed in an easily visible location on the website.	☐
		If the website can be viewed in multiple languages, the privacy notice has been translated into these languages.	☐
		If we have General Terms and Conditions (AGB) available, these have been reviewed to ensure they comply with data protection rules.	☐
		If a newsletter is sent out, this has been reviewed to ensure it complies with data protection rules.	☐
No. 2	**Review/conclusion of contracts in the case of data processing by third parties (incl. transfer of data abroad)** Examples: Contracts with IT service providers concerning the outsourcing of data processing via cloud technology, or contracts with service providers that handle the payroll for employees of the staffing service provider. Under the revFADP, the processing of personal data can be assigned to third parties through an agreement or the law, as long as the data is processed in the same way as the staffing service provider itself would be permitted to do and there is no legal or contractual confidentiality obligation that would prevent outsourcing. In addition, the contracting company must ensure that the contracted third party ensures data security (Article 9 (1) and (2)	Contracts with service providers have been checked for compliance with data protection rules.	☐
		The EU Standard Contractual Clauses or other suitable guarantees have been agreed upon with service providers based in countries that do not have adequate data protection regulations, and additional measures have been taken if necessary.	☐

	revFADP). Now, the data processor may only assign the processing to a third party with the prior approval of the data controller (right to veto) (Article 9 (3) revFADP). The data processor must report any data security breaches to the controller as quickly as possible (Article 24 (3) revFADP). The staffing service provider (outsourcer) remains responsible for the data processing and continues to act as the data controller. When data is disclosed abroad, steps must be taken to ensure that the personality rights of the data subjects are not infringed upon.		
No. 3	**Review whether data protection principles are being observed** These are legitimacy, purpose limitation, good faith, proportionality, data integrity, consent if applicable, data security, privacy by design, and privacy by default.	Checks have been made to ensure compliance with these principles when processing personal data.	☐
		Compliance with data security requirements has been ensured.	☐
		Checks have been made to ascertain whether consent is required and that it has been granted if so.	☐
		The principles of privacy by design and privacy by default are being sufficiently followed.	☐
No. 4	**Development of process for reporting any data security breaches**	A process has been developed that stipulates how to respond in the event of a data security incident as quickly as possible and how the incident is to be reported to the Federal Data Protection and Information Commissioner (FDPIC) and, if applicable, the data subjects.	☐
No. 5	**Development of process in the event of requests by data subjects**	There is a process stipulating how to act in the event of requests by data subjects to ensure data subjects obtain the necessary information required to assert their rights and ensure data processing is transparent.	☐

		As a rule, this information must be provided within 30 days.	
No. 6	**Compliance with formal obligations**	A central point of contact has been appointed for all data protection issues (e.g. legal service, IT); if necessary, a data protection advisor with the necessary expertise has been appointed in accordance with Article 10 revFADP. This advisor must also be professionally independent and not subject to the instructions of the data controller, and they must not engage in any activities that are incompatible with their duties.	☐
		If necessary, a register of data processing activities has been created.	☐
		If necessary, a data protection impact assessment (DPIA) has been carried out.	☐
		Employees have been trained in the requirements of the revFADP and the measures taken within the company.	☐
		Insofar as automated processing of particularly sensitive data is being carried out on a large scale or high-risk profiling is taking place and the preventive measures do not ensure data security, mandatory recordkeeping obligations are observed.	☐

swissstaffing

EXAMPLE 1: CONSENT CLAUSE TEMPLATE

[*This template is incomplete and for demonstration purposes only. It should be adapted to the individual circumstances.*]

Application documents are treated with the strictest confidentiality and are only used for their agreed purpose.

- Recruitment: Data is only processed insofar and for as long as it is required for recruitment purposes. Data may be shared with potential employers.
- Staff leasing: Data continues to be processed until the leasing relationship comes to an end and profiles may be shared with (potential) contracting companies.

The application file, whether analog or digital, will be deleted/destroyed without your consent at the end of the application process, provided there is no legal obligation to retain it.

I hereby expressly consent to my personal data being processed, stored and forwarded in the following way:

☐ I consent to [staffing service provider] storing, processing or forwarding my personal data, which I have provided in connection with my application, within the companies of [staffing service provider] in Switzerland and abroad [if no adequate data protection: state country name] for the purpose of staff leasing and/or recruitment.

☐ I consent to the personal data, which I have provided in connection with my application, being stored, processed and disclosed to third parties in Switzerland and abroad for the purposes of staff leasing and/or recruitment, both during the leasing or recruitment process and beyond the end of the specific leasing or recruitment process. These third parties include the companies and service providers connected to [staffing service provider] that provide and manage the IT applications used, as well as other companies that are involved in helping [staffing service provider] with the procedures required to provide its contractual services (e.g. payroll service providers). In this respect, I also consent to my data being transferred to countries [state country name] where there is no adequate level of data protection. Insofar as I have provided particularly sensitive personal data pursuant to Article 5 (c) revFADP as part of my application (e.g. a photo showing my ethnic heritage, etc.), my consent also covers this data.

☐ I consent to [staffing service provider] sending newsletters to the email address I have provided. These newsletters contain information about job vacancies that I may find interesting.

Each instance of consent provided has been made willingly and independently of the others. I can withdraw my consent to any of these things at any time without giving a reason and have the right to request the erasure of my personal data at any time. A link can be found at the end of each newsletter allowing me to unsubscribe. I acknowledge that, if I withdraw consent for my personal data to be processed (with the exception of the consent to receive the email newsletter), [staffing service provider] will no longer be able to provide the services offered and thus our underlying contractual relationship will come to an end.

swissstaffing

EXAMPLE 2: SAMPLE DATA PROTECTION AND CONSENT CLAUSE IN GENERAL TERMS AND CONDITIONS

[*This template is incomplete and for demonstration purposes only. It should be adapted to the individual circumstances.*]

Data protection

The parties undertake to comply with the relevant data protection regulations at all times. As part of the respective contract, [staffing service provider] is entitled to collect, process and use and disclose the data of the client's employees, directors and other staff (hereinafter referred to as the client's "Personal Data") for all purposes related to the performance of the contract. This includes transferring the client's personal data abroad [if no adequate data protection: state country name] for the aforementioned purposes, which may be necessary for the fulfillment of the contract. Furthermore, [staffing service provider] is expressly authorized to process the client's personal data in any form and disclose it to any affiliate companies or third parties abroad.

The client hereby grants their consent to the use of their personal data for marketing purposes. The customer expressly declares that the data subject provides their consent. [Staffing service provider] may request this from the customer at any time.

swissstaffing

EXAMPLE 3: SAMPLE COMMISSIONED DATA PROCESSING CLAUSE IN GENERAL TERMS AND CONDITIONS

[*This sample clause is incomplete and for demonstration purposes only. It should be adapted to the individual circumstances.*]

Processing of personal data via third parties (commissioned data processing)

The contractor undertakes to process personal data from the [staffing service provider] that it is forwarded or has access to only to the extent and for the purposes necessary for the performance of the contract.

The contractor undertakes to take appropriate technical and organizational measures to ensure data protection and information security.

The contractor will only process personal data (incl. access and web server location) in Switzerland or the EU, or in the European Economic Area.

The contractor will disclose at least those subcontractors who process personal data on its behalf before the contract is concluded. The contractor will bind all subcontractors, agents, and third parties involved to the obligations arising from this commissioned data processing contract. The contractor must obtain the prior written consent of [staffing service provider] before involving each additional subcontractor. If there is no written consent, the contractor may not make use of any additional subcontractors. It is at the sole discretion of the client whether to accept or reject any third party as a future subcontractor.

The contractor will handle all personal data that it receives directly or indirectly in connection with the contract with confidentiality. Specifically, the contractor assures [staffing service provider] that it will neither pass on the personal data to unauthorized third parties nor make it accessible to unauthorized third parties in any other form. The contractor will ensure that all subcontractors, agents, and third parties involved are bound by this confidentiality obligation.

The contractor will help [staffing service provider] comply with the requirements of the applicable data protection regulations. Specifically, it will duly answer all the client's questions concerning the processing of personal data without delay. It will forward requests from data subjects or authorities to [staffing service provider] without delay, without answering them itself. The contractor is obligated to cooperate with any proceedings instigated by supervisory authorities that relate to the services it provides, and will provide any information and documents requested.

The contractor will immediately inform [staffing service provider] if it knows or suspects that any personal data that it processes for [staffing service provider] has been or could be exposed to unauthorized access, disclosed to unauthorized third parties, lost or damaged, or processed in any other way in breach of the law or the contract. The contractor will immediately take any measures necessary to ensure personal data is secure and prevent or mitigate any potential negative consequences.

[Staffing service provider] has the right to verify whether the contractor is complying with the applicable data protection regulations at any time.

Upon termination of the contract, the contractor must transfer to [staffing service provider] or destroy the personal data (including any copies) that it has processed for [staffing service provider], subject to any other contractual provision, in accordance with the express instructions of [staffing service provider]. The contractor must document the destruction of this data and provide [staffing service provider] with a copy of this documentation unprompted.

ANNEX: USEFUL LINKS

Communication on the legislation regarding the total revision of the Federal Act on Data Protection and the amendment of other data protection directives from September 15, 2017; you can find the document here (in German)

Press releases from the Federal Office of Justice can be found here and here (in German)

The general website of the Federal Data Protection and Information Commissioner (FDPIC) can be found here

Guidelines on the technical and organizational measures (2015) of the FDPIC can be found here

The form for preparing a data protection impact assessment for the Canton of Zurich can be found here (in German)