Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissoner (FDPIC)

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

GUIDE

by the data protection authorities of the Confederation and the Cantons

on the application of data protection laws to the digital processing of personal data in connection with elections and voting in Switzerland

Status: 1 December 2018

The guide has been produced in collaboration with the experts
Urs Maurer-Lambrou, attorney-at-law, LL.M., und Prof. Dr. Adrian Vatter, political scientist

In order to promote general comprehensibility, this document does not contain any specific legal references.

Feldeggweg 1, 3003 Bern
Tel. +41 58 463 74 84, Fax +41 58 465 99 96
www.edoeb.admin.ch

Contents

1 Why this guide and who is it for? 3

2 Political parties and interest groups 4

3 Public registers 4

4 Data processing 5

4.1 Procurement 5

4.2 Analysis 5

4.3 Targeting with information 6

5 Further actors in data processing 6

5.1 Data dealers 6

5.2 Data analysis companies 7

5.3 Data platforms 7

5.4 Individuals (addressees/recipients) 7

6 General legal data processing principles 8

7 Right of voters to transparency 9

8 Summary overview 11

1 Why this guide and who is it for?

The digital society is a reality in which elections and voting take place at all levels of the Swiss Confederation. New data processing phenomena which can have an impact on voting behaviour are constantly appearing. Online communication offers those involved in shaping political opinion the opportunity to send messages quickly and cost-effectively to voters, or to enter into dialogue with them; this is especially true where voters avoid traditional media for cost or other reasons and primarily use the internet for their information requirements and social exchange.

In e-commerce, large amounts of personal data are obtained and processed automatically. This data is analysed in order to send personalised advertising messages to customers, offering them goods and services that match their profile. The automated data processing methods of big data, analytics, profile building and micro-targeting are also used to send messages to voters in which parties and interest groups seek to influence political opinion in the run-up to votes and elections.

Where private individuals or federal authorities that use these data processing methods make reference to identifiable persons, they are subject to the Federal Act on Data Protection (FADP) and the supervisory activities of the Federal Data Protection and Information Commissioner (FDPIC). Where cantonal or communal authorities that organise elections and votes use these data processing methods, they are subject to cantonal data protection legislation and local data protection supervision. This is why this guide has been authored jointly by the FDPIC and the Conference of Cantonal Data Protection Officers (PRIVATIM).

The Federal Constitution guarantees political rights and the freedom of citizens to form their own opinions and give genuine expression to their will. The data protection authorities help to ensure that the political process complies with the Constitution by encouraging those involved to respect individuals' right to privacy and to make their own decisions on information.

Anyone who processes data in the context of elections and voting should be aware that data protection law assumes that information on political and ideological views is subject to a higher level of protection than comparable data in a commercial environment.

The data protection authorities have drafted this guide because they have a statutory duty to advise private individuals and public bodies and to inform the public about the systemic risks of processing personal data. It should be understood as an aid to interpretation: the FADP dates from 1992 but governs data processing in the context of elections and votes in the dynamic environment of digitalisation. It is aimed at all those involved in shaping political opinion and aims to encourage them to make digital processing methods recognisable and comprehensible. It should however be pointed out that there are two topical issues which do not fall within the ambit of this guide: the issue of the whether apparent factual statements are true or not, which is the subject of public debate under the catchword "fake news" and which is not subject to the data protection legislation; and the issue of electronic voting in Switzerland.

2 Political parties and interest groups

Data processing in the political process and the associated legitimate objective of influencing political opinion is primarily an activity of political parties and interest groups. Normally these parties and groups take the form of private associations or foundations that pursue political, religious, social, scientific and other ideological purposes.

Although there is no comprehensive case law on this subject, it can be assumed that digital data processing in connection with the political process is generally subject to the level of protection applicable to particularly sensitive personal data simply because of its purpose of influencing the ideological views of many people. This is particularly the case if automated analysis methods are used which compare a large volume of sensitive or non-sensitive data in order to create personality profiles, which, according to the Federal Administrative Court in the Moneyhouse case[1], also means that the persons concerned are entitled to increased protection. As private "owners" of data collections, political parties and interest groups must thus comply with their overall responsibility for the acquisition, storage, maintenance and further use of the data processed there (see Table A). They are guided by the fundamental principle of transparency (Chapter 7). If the parties and interest groups permit voters to see which processing methods they apply, they may meet with acceptance.

In the context of the political process, parties and interest groups are free to use third parties to process data by transferring all or part of the process to such parties or by obtaining data from third parties. As part of their overall responsibility as owners, they must disclose the involvement and roles of these third parties, regardless of whether these are owners or only contractors. They must ensure that the latter comply with the provisions of data protection legislation (see Table C).

3 Public registers

The cantons keep a register of voters - the electoral roll. The electoral roll is based on data held by the residents' registration office. Persons moving in and out of any commune are required by law to register and deregister with the commune by presenting proof in the form of official documents. The residents' registration office therefore determines when the right of a person to vote in that specific commune begins and ends, and duly records this on the electoral roll. The electoral rolls form the basis for voting rights in federal, cantonal and communal elections and votes. Federal law stipulates that the electoral roll is open for inspection by voters. The cantons determine the form in which voters may exercise their right to inspect the roll (on-site inspection, publication on paper, publication online). They also determine whether and in what form access to the residents' register is granted.

Some cantons combine the communal residents' registers into a register of all inhabitants of the canton. Often additional data is added to these central registers (e.g. e-mail addresses and mobile phone numbers from tax returns).

As part of their overall responsibility as holders of state data files, the authorities responsible for the public registers must ensure that the data they contain is kept secure and only passed on to third parties if this is legally permissible. They must guarantee that no improper uses or uncontrolled data flows can occur (see Table B).

[1] Federal Administrative Court (FAC) Decision A-4232/2015 of 18 April 2017

The technical and organisational measures used by the authorities to protect these central files vary. Address and contact data are personal data that are subject to data protection legislation but are not particularly worthy of protection.

Cantonal law may provide that the residents' registration offices of the communes may disclose residents' address data subject to certain criteria (i.e. in lists, e.g. of young citizens) if requested to do so. As a rule, these lists may only be used by the person making the request for specific, often non-commercial purposes and may not be passed on to third parties. The commune checks whether the legal requirements for disclosure have been met and if so can pass on the data to the applicant. Normally local residents who wish to protect their personal data in the residents' register can refuse to have their data published on a list or passed on to third parties. This presupposes that the commune informs its residents of the conditions and extent of disclosure and of the option of refusal. So far, it has been rare for the authorities to offer specific options for refusing political advertising. In practice, attempts are being made to take appropriate measures to ensure that protective measures such as the right to refuse to disclose data in the residents' register or the electoral register cannot simply be circumvented by inspecting another register.

4 Data processing

According to the legal definition, data processing is any handling of data, regardless of the means and procedures used. In the context of elections and votes, data processing can be divided into the procurement, analysis and allocation of information.

4.1 Procurement

In the political process, parties and interest groups firstly have access to data they have acquired themselves, such as party members' addresses or e-mail address lists of newsletter subscribers. Often this data is supplemented by information that the parties and interest groups obtain when collecting signatures for initiatives or referendums or when speaking to members of the public at events, during door-to door campaigning or on the telephone. In addition, they can obtain data from publicly accessible sources such as telephone directories or public registers.

Internet portals or statistical websites can be used to collect data with the help of web mining, by commissioning third parties to obtain the data or simply by purchasing the information. Web crawler services can systematically search for website content or e-mail addresses and obtain the information they want. Data platforms are another possible source of data.

4.2 Analysis

Under the heading of 'big data', large quantities of heterogeneous data are processed over a longer period of time in the e-commerce sector, i.e. they are compiled for analysis purposes. With the help of powerful computer systems and analysis methods, data can be evaluated and the interests of individuals or small groups of similarly thinking people can be identified. Statistical models can be used to predict which products or services are suitable for which profile groups of existing or new customers (predictive analytics). Existing or potential customers are then sent advertising messages tailored to their profile or, for example, are sent suitable product recommendations for an online shop.

In a political context, profile building aims to ensure that each profile group not only differs from other groups in its common interests, but also that the people within these groups are more similar in their political positions and ideas than people from different groups.

Segmentation based on demographic, ideological, socio-economic and psychological characteristics and various methods of artificial intelligence are used to predict the behaviour of the individuals concerned and to target them with political messages.

When compiling data, the owners of a data collection must be aware that a large volume of sensitive - i.e. particularly sensitive - or even ostensibly insensitive data can condense into personality profiles as defined in the Data Protection Act. These are subject to qualified or stricter legal protection. The Federal Administrative Court has issued a detailed ruling on this subject in its Moneyhouse judgment (Chapter 2). Qualified protection also applies to the processing of sensitive data such as that on ideological or political views, which the legislator has placed under special protection (Chapter 7).

4.3 Targeting with information

Based on the assumption that people in a common profile group react particularly strongly to certain messages, individual groups are given targeted information via e-mail distribution lists or social media. With this approach, political parties and interest groups seek to influence political opinion in the run-up to votes and elections. In so-called micro-targeting, not only the content of messages, but also the way in which they are addressed are individualised. This presupposes that the information about the target persons based on the collected data is so precise that appropriate political messages can be conveyed via their preferred communication channels.

Micro-targeting can have the desired influential effect, particularly in the case of referendums, where experience shows that a large number of voters do not yet have a firm opinion on a particular topic. In elections under a system of proportional representation, such as the elections to the National Council, on the other hand, an established pattern of electoral behaviour based on tradition and custom is often observed. The situation can be different in elections to the Council of States where candidates campaign across party lines.

Personalised messages in a political context do not necessarily aim to influence who or what a person votes for. Sometimes they can serve to encourage a person to vote or to inhibit them from doing so, depending on whether the evaluated data identify the person concerned as a political friend or opponent. A further possibility is simply to encourage people to vote, but to send the message selectively - and not to suspected political opponents.

5 Further actors in data processing

5.1 Data dealers

Commercial address traders and providers of similar services procure information of all kinds, which they process and market systematically, structured as far as possible according to personal characteristics. The data offered originates from a multitude of applications, registrations, orders and declarations

that have been filled out when ordering goods and services, accepting business conditions or taking part in competitions. Information published by public authorities such as statistics on election results or levels of unemployment, as well as public announcements, commercial registers and lists of debtors are also used as data sources. Data are also collected in consumer surveys or by evaluating generally available sources. By combining data from different sources, these commercial providers supplement private addresses, for example, with additional information such as consumer behaviour, socio-demographics or living conditions.

Private data merchants process personal data in the context of the political process as data owners with overall responsibility (see Table A) or as data processing contractors (see Table C).

5.2 Data analysis companies

Data analysis companies can be contracted to manage and analyse data held by political parties or lobby groups. They may be, for example, communication agencies or other companies that specialise in certain analysis procedures (e.g. website analysis, crawler agencies).

At the same time, data analysis companies can also be data traders which, for their own (commercial) purposes, obtain information from various sources, evaluate it and then make it available to interested groups for a fee.

Data analysis companies process personal data in the context of the political process as the data owner with overall responsibility (see Table A) or as the data processing contractor (see Table C).

5.3 Data platforms

Data platforms of search engine operators such as Google or social networks such as Facebook or Twitter collect the personal data such as name, gender and age that registered users have provided. In addition, extensive data are automatically recorded when registered and other users visit these data platforms.

This includes technical data such as IP addresses or device numbers and information about pages marked with “Like", shared messages, etc. In addition, information is collected from external websites or apps that are linked to these platforms on the basis of advertising partnerships.

Where private data platforms process personal data in the context of the political process as data owners with overall responsibility, the information in Table A and Table D applies. Where they process or pass on such data as data processing contractors, Table C provides the relevant information.

5.4 Individuals (addressees/recipients)

The electorate is the addressee of information processed for the purpose of shaping political opinion in the run-up to elections and ballots. While political advertising on the radio and television is prohibited in Switzerland and print media convey political advertisements without prior interaction with individual readers, data platforms offer the possibility of conveying political messages to individual persons or groups of persons in a targeted manner. These persons or groups can then comment on and dissemi-

nate the messages they receive. By communicating with billions of users on the world's largest platforms, not only network operators but also their customers accumulate large quantities of address, text, sound and image data relating to families, friends and acquaintances, allowing conclusions to be drawn about their worldview and political preferences. This information, together with the associated user accounts, is stored in the platform operators' data centres and in some cases on users' smartphones and computers. Through targeted distribution or public dissemination, they enable themselves and third parties to influence political opinion and the electoral or voting behaviour of other persons. Like the professional owners of data collections, individual addressees as private individuals thus also bear responsibility for their processing of personal data in a political context (see Table E). To be able to meet this responsibility, they must first be aware of this fact.

6 General legal data processing principles

Anyone who processes personal data in the context of elections and votes must observe the general principles of data protection legislation:

The term 'personal data' is defined as any data relating to an identified or identifiable person. Data that allow conclusions to be drawn about political or ideological views are considered particularly worthy of protection, so that their processing is specially protected by law. The further processing of data which are not sensitive in themselves through procedures such as data analysis or enhancement may give rise to particularly sensitive personal data or personality profiles, which in turn are specially protected by law in accordance with the legal precedent set by the Federal Administrative Court in the Moneyhouse case (Chapter 2).

Personal data must first be processed in good faith. This means that the data must not be collected and processed in a way that the data subject would not have expected in the circumstances and that they would probably not agree with. Data subjects must be able to recognise that their data is being collected and processed. They must also be able to identify the purpose for which their data is being processed, who is processing the data and - if the data are passed on to third parties - the categories of possible data recipients. Data subjects must also be able to see when their personal data is collected from third parties, such as data handlers.

In addition, the principle of proportionality also applies to the processing with regard to the quantity of personal data processed and the duration of processing. For processing to be proportionate, a data processor may only process data that is suitable and objectively necessary in order to achieve a (legitimate) goal. In the processing of the data, the objective pursued and the means used must be in reasonable proportion to one another and the rights of the data subjects must be safeguarded. Data processing must be reasonable for the data subjects, both in terms of its purpose and the means by which it is carried out.

According to the principle of purpose limitation, personal data may only be processed for the purpose stated when it was collected, which must be apparent from the circumstances or must be provided for by law. Without specific justification, data may not be processed in a manner incompatible with these purposes.

Anyone who has a data collection must also ensure the accuracy of the data that it contains, insofar as the data relates to people. The data processor must take all reasonable measures to ensure that personal data are corrected or destroyed if, when taking account of the purpose for which they have been collected or processed, they are inaccurate or incomplete. Purely factual data that make no reference to specific or identifiable persons are not subject to data protection law; from this it follows that the truthfulness of political facts and the problem of so-called "fake news" are not a matter of data protection law.

Finally, according to the principle of data security, personal data must be protected through suitable technical and organisational measures against unauthorised processing. It is not only the owner of a data collection who is required to protect personal data; every data processor must do so, even if the personal data concerned does not constitute a data collection. This obligation therefore applies to anyone who processes personal data in the context of elections and votes. The specific data protection, organisational and technical risks must be assessed and appropriate protective measures taken. This requires internal documentation that shows how the above obligations are fulfilled with regard to the different categories of data processed.

7 Right of voters to transparency

Persons processing data must also be aware of the particular relevance of the principle of transparency. This gives voters the right under data protection law to know which digital processing methods and technologies are being used to target them and to influence their political views.

State bodies that make data available in the context of elections and votes fulfil this transparency requirement by complying with a framework of publicly accessible legal principles.

The processing of personal data by private entities such as political parties or lobby groups may be based on the consent of the persons concerned, or on an overriding private or a public interest. In practice, in a political context, only the consent of the data subjects is sufficient in most cases. This consent is only valid if it is given voluntarily and is adequately informed. As explained above, in a political context, the personal data processed normally relate to political or ideological views and fall into the category of particularly sensitive personal data. Personality profiles can be created by linking the data that the data subjects leave behind on websites and social platforms, for example. In a political context, data about persons may thus be processed if they have given their express, self-determined and informed consented to their use.

Those seeking to shape political opinion process are allowed to process data only for the purposes, to the extent and with the methods for which consent has been given. Express consent is given in particular if the data subjects have registered themselves on the website of a political party, for example, and expressly consent (e.g. by ticking the appropriate box) to their data being processed accordingly. Declarations by which individuals accept terms of use in only a general manner, however, do not constitute express consent. The same applies to the terms that people agree to on social media platforms, in order to subscribe to the service or comment on the concerns that are raised or on other content. In addition, a person can only consent to the use of their own data. The processing of the data of third parties requires the consent of the persons concerned.

Consent is self-determined if the persons concerned can agree to the activation or deactivation of individual aspects and functionalities of the digital applications (e.g. by ticking the appropriate boxes) and thus have a genuine choice, not only as to whether, but also as to what extent they make their data

available. In addition, data subjects must at all times be able to revoke their consent and demand that their data be deleted. In order to meet these requirements, the website operators concerned must invest in data protection technologies.

'Informed consent' presupposes that the persons concerned are given full and fair notice before registration that their data will be processed and of how the analysis methods used for this purpose, including automated programs and artificial intelligence, work. They must also be informed of their rights, such as their right to revoke their consent at any time. 'Fair' means that the information is easy to understand, quick to find and clearly communicated. Online texts are 'complete' if they explain the purposes and effects of digital processing methods and technologies in a manner appropriate to the addressees and, in particular, provide information on the duration of processing and the possible passing on of the data. The information begins with a clearly visible summary on the registration page, which explains the most important points of data processing. Each of these points contains further links that lead the reader to the relevant passages of the processing regulations and data protection provisions. In a political context in particular, fair information means that those concerned are not deceived by misleading or false information about senders and sources or, in the case of communications sent to individuals, left in the dark as to whether they are interacting with a human being or a computer program. They must also be able to tell whether the information they are sent online is personalised or not intended for anyone in particular. If necessary, it must be clear from the terms of use which technologies or procedures are being used and what criteria apply to the personalised messages that are sent. Complete information also includes information on the processing of data enhanced and evaluated with information from social media.

8 Summary overview

A **Parties and lobby groups**	Where parties and lobby groups assume overall responsibility as a data file owner (Chapter 2), they must take the following information into account: • Processing must be carried out ***lawfully*** and in accordance with the general principles of the Data Protection Act, irrespective of the involvement of third parties (Chapter 6). • ***Authorised third parties*** are required to provide evidence that they are taking appropriate organisational and technical measures for data security (Chapter 6). • The right of voters to ***transparency*** (Chapter 7) is fulfilled by ***website supported information*** on - the identity of the holders of the collection; - the categories of data processed; - the collection of data from third party sources; - the current purpose of and reason for processing; - the methods of processing, including the purpose and methods of analysis, including artificial intelligence; - the categories of any data recipients; - the roles, obligations and responsibilities of data providers, data analysis companies or data platforms; - the relevant terms of use of third parties and their sources. • Processing takes place in compliance with the principles of ***purpose limitation*** (Chapter 6) and ***proportionality*** (Chapter 6), according to which any further processing must always be for the purpose underlying the procurement and must stop when this purpose is achieved; • Any ***consent*** required for processing personal data in the context of the political process is expressly obtained (Chapter 7); • The ***accuracy of the data*** is guaranteed even if third parties are involved and data that are no longer required are deleted (Chapter 6); • The data protection, ***organisational and technical risks are assessed*** and appropriate protective measures taken (Chapter 6); • Internal ***documentation*** exists showing how the security of the various categories of processed data is guaranteed (Chapter 6); • The data subjects' ***rights to information*** as well as any notification obligations for data collections or information obligations for the transfer of personal data abroad to the data protection authorities are observed.
B	Authorities responsible for the operation of the **residents' register and electoral roll** (Chapter 3) must ensure that

Voting rights registers	• the data processing does not go beyond the ***legal requirements*** with regard to purpose, content, scope and duration; • personal data is only passed on where there is an express legal basis for doing so, or the data has previously been anonymised; • citizens can refuse to have their data passed on for the purposes of political advertising where this is not excluded by law in advance; • the ***risks*** to technical and organisational security are ***assessed and documented***, including re-identification risks, and the necessary protective measures are taken (Chapter 6); • data losses are reported to the data protection authorities within a reasonable time.
C **Data Dealers and Data Analysis Companies**	Where private data dealers (Section 5.1) or data analysis companies (Section 5.2) process data in the context of the political process as the ***owner*** with overall responsibility, they must take account of the information in Table A. Where they act as ***contractors*** and process data in the context of the political process • before concluding a contract, they must make sure that their client is willing and technically and organisationally able to use the information in question in accordance with the law and the contract; • they must comply with the rules in the Moneyhouse decision (Chapter 2) on combining data from different sources to create profiles (Section 4.2); • they must ensure data security by assessing and documenting risks and taking the necessary protective measures (Chapter 6); • they must support their clients at their request in risk assessments and notify them of any loss of data. They must explain in their terms of use or written contractual conditions: • how, from which sources, with which methods and for what purposes they have obtained the data passed on; • whether and, if so, for what purposes and in what form the persons concerned were able to consent to the data being passed on and processed.
D **Data platforms**	Irrespective of whether data platforms (Section 5.3) process information in the context of the political process as the owner with overall responsibility or as an agent, processing is generally governed by ***general terms and conditions of business and use***. • They must respect the right of voters to ***transparent data processing*** (Chapter 7) and therefore continuously invest in ***data protection-friendly technology*** in order to offer users multi-level ***information*** and ***genuine, user-friendly digital options***. • They must provide the data protection authorities with details of suitably informed and authorised ***contact persons*** who can

	provide information in the event of data loss or other data protection-relevant incidents that have potential consequences for elections and votes. Where data platforms process information as the ***owner*** with overall responsibility, they must also comply with the rules in Table A. Where they process data on a ***contractual basis***, they must also comply with the rules in Table C
E **Individuals**	Before private individuals publish, evaluate or disseminate political content and statements on social networks, they must take care to protect the privacy and other personal rights such as the reputation or family life of those concerned. Before ***forwarding information*** relating to their friends, family members or other identifiable persons to parties, lobby groups, data traders, data analysis companies or data platforms, private individuals must obtain the **express *prior consent*** of the persons concerned. They must ensure that any software that accesses this data comes from a reliable source.