Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissioner

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

Status: December 15, 2022[1]

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

In the interests of general comprehensibility, this document does not contain any specific legal references.

[1] This update replaces the version of June 1, 2019

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Contents

1 What is this guide about? ... 4

2 Competent supervisory authorities and applicable law ... 4

3 Addressees and purpose of the guide ... 4

4 Players ... 5

4.1 Political parties and interest groups ... 5

4.2 Data controllers or processors ... 5

4.3 Public registers ... 6

4.4 Data analysis companies ... 6

4.5 Data dealers ... 7

4.6 Data platforms ... 7

4.7 Individuals ... 7

5 Personal data in the context of elections and votes ... 8

5.1 Personal data ... 8

5.2 Sensitive personal data and personality profiles ... 8

6 Processing principles ... 8

6.1 Good faith and transparency ... 9

6.2 Proportionality ... 9

6.3 Purpose limitation ... 9

6.4 Data accuracy ... 9

6.5 Data security ... 9

7 Breach of personality rights and grounds of justification ... 10

7.1 Breach of personality rights ... 10

7.2 Overriding private or public interest ... 10

7.3 Consent ... 11

7.4 Express consent ... 11

8 Data processing in a political context 12
8.1 Data collection 12
8.2 Data analysis 13
8.3 Information targeting 13
8.4 Addressing of data subjects 14
8.5 Consent 14
8.6 Rights of data subjects 14
9 Requirements for websites 14
10 Practical examples 15
Example 1 15
Example 2 16
11 Summary overview 17

1 What is this guide about?

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.

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 – and therefore that they must meet even more stringent requirements.

2 Competent supervisory authorities and applicable law

Where processing methods make reference to identified or 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 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 guide has therefore been authored jointly by the FDPIC and the Conference of Cantonal Data Protection Officers (privatim).

On 1 September 2023 – shortly before the general election to the Federal Assembly – the totally revised Federal Act of 25 September 2020 on Data Protection and its associated ordinances will come into force. More information on this can be found in our publication 'The new Data Protection Act from the FDPIC's perspective'. A number of cantonal data protection laws are also currently being revised (see Section 8.1 below).

3 Addressees and purpose of the guide

This guide is addressed at all political parties and others involved in the formation of political opinion.

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. The guide aims to provide the addressees with an aid to interpreting applicable federal and cantonal data protection law so that they can assess which processing methods for shaping political opinion in the digital sphere are, in the view of the data protection authorities, permissible under data protection legislation and which requirements must be met.

The guide aims to encourage those involved in shaping political opinion to make digital processing methods recognisable and comprehensible for voters. 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 whether apparent factual statements are true or not, which is the subject of public debate under the catchword 'fake news' and which is not the object of data protection legislation; and the issue of electronic voting in Switzerland.

4 Players

4.1 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.

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 them.

Political parties and interest groups, as 'controllers' or 'private controllers of data files', thus remain responsible for the collection, storage, maintenance and further use of any data processed by the third parties (see Table A).

4.2 Data controllers or processors

Under current data protection legislation, personal data can be processed in two different roles: as the controller of the data file or as the commissioned (data) processor. A data controller is a private person or entity or a public authority that alone or together with others decides on the purpose and means of processing (see Table A). A data processor is a private person or entity or public authority that processes personal data on behalf of the data controller (see Table C).
The data controller is responsible for ensuring compliance with provisions on data protection, even when the processing of personal data is entrusted to a third party (the data processor). Joint responsibility of several data processors is also possible.

Example: Voter A goes to the website of a political party and looks at its manifesto, but does not join the party.

The party would like to directly target on social media voters who have been on its website, but who have not joined the party, i.e. those such as Voter A. It has therefore integrated a plug-in known as a tracking pixel into its website. When a voter visits the party's website, the browser automatically establishes a link to social media servers and sends a host of information about the voter to the social media platforms. In this way, the social media companies can, as a rule, monitor when an individual visits a website, and use this information for a specific purpose, e.g. placing the voter in a specific advertising target group. As a result, when Voter A subsequently goes on social media, they will see advertising for the party.

The political party and the social media companies are joint data controllers.

If a data processor is located in a third country that is considered insecure in data protection terms, special measures must be taken. This may be the case when personal data is stored on a server in the US. Further information is published on the FDPIC website (link: Transborder data flows (admin.ch)).

4.3 Public registers

The communes keep a register of voters – the electoral roll. The electoral roll is based on data held by the residents' registration office. Persons moving to or from a commune are required by law to officially register and deregister with the commune. 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 voters may inspect the electoral roll. 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. email addresses and mobile phone numbers from tax returns).

As part of their overall responsibility as controllers 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).

The technical and organisational measures used by the authorities to protect these core data files vary. Address and contact data is personal data that is subject to data protection legislation but is not sensitive.

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 this is the case, 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 roll cannot simply be circumvented by inspecting another register.

4.4 Data analysis companies

Data analysis companies can act as an agent or representative and assume the management and analysis of the parties' or interest groups' data. These may be communications agencies or other companies that specialise in specific analysis methods (e.g. website analysis, crawler agencies).

Data analysis companies may also be data dealers that independently obtain information from a range of sources, assess it and then make it available to interested groups for a fee.

Private data dealers may process personal data in the context of the political process as controllers of data files (see notes in Table A) or as third-party processors (see Table C).

4.5 Data dealers

Commercial address dealers and providers of similar services collect information of all kinds, which they process and market systematically, structured as far as possible according to personal characteristics. The data provided 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 is 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 dealers process personal data in the context of the political process as data file controllers (see Table A) or as third-party processors (see Table C).

4.6 Data platforms

Data platforms of search engine operators such as Google or social networks such as Facebook or Twitter collect the personal data that registered users provide, such as their name, gender and age. In addition, extensive data is automatically recorded when registered users and others 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.
Other platforms that specialise in collecting signatures for votes harvest large amounts of contact data including email addresses, postal addresses and information about political preferences. The platforms are either managed by the parties or interest groups themselves or make their services and data available to interested parties as third-party providers.

Where private data platforms process personal data in the context of the political process as data controllers, the information in Table A and Table D applies. Where they process or pass on such data as third-party data processors, the information in Table C applies.

4.7 Individuals

Information processed for the purpose of shaping political opinion in the run-up to elections and ballots is addressed at voters. 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 disseminate 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 of this information, they and third parties can influence political opinion and the voting behaviour of other persons. Like the professional controllers of data files, private individuals thus also bear responsibility for processing personal data in a political context (see Table E). To be able to meet this responsibility, they must first be aware of this fact.

5 Personal data in the context of elections and votes

5.1 Personal data

The term 'personal data' is defined as any data relating to an identified or identifiable person. Purely factual data that does not relate to identified or identifiable persons does not fall under the scope of data protection law, which means that the veracity of political factual content and the issue of voters being influenced by 'fake news' is not relevant to the issue of data protection. With regard to incorrect factual content having a demonstrably detrimental effect on the personality rights and reputation of individual persons, reference is made to the relevant provisions of the Swiss Civil Code and of the Swiss Criminal Code (esp. Art. 28 Civil Code and Art. 173 ff. and Art. 261bis Criminal Code).

5.2 Sensitive personal data and personality profiles

Data that allows conclusions to be drawn about political or ideological views are considered sensitive, and so the processing of such data is subject to special legal requirements. The further processing of non-sensitive data in procedures such as data analysis or enhancement may generate sensitive personal data or personality profiles, which in turn are sensitive in accordance with the legal precedent set by the Federal Administrative Court in the Moneyhouse case (Section 2).

Although there is no comprehensive precedent on this issue, it can be assumed that digital processing in connection with the political process, for the reason alone that its purpose is to attempt to influence many people's ideological views, should as a rule be subject to the degree of protection applicable to sensitive personal data. This is particularly the case when automated analysis methods are used which compare a large amount of sensitive or non-sensitive data in order to create personality profiles which, according to the decision of the Federal Administrative Court in the Moneyhouse case, require a greater level of protection for the data subjects.[2]

6 Processing principles

Anyone who processes personal data in the context of elections and votes must observe the general processing principles of data protection legislation. In addition, public authorities are bound by the principle of legality, according to which there must be an adequate legal basis for the processing of any personal data.

[2] FAC decision A-4232/2015 of 18 April 2017

6.1 Good faith and transparency

Personal data must first be processed in good faith. This means that it may 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.

The transparency principle requires that data subjects 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 processed, who processes the data and – if the data is 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 dealers. Only then is it clear to voters which digital processing methods and technologies are used to address and influence them. By making it sufficiently clear which data processing methods they use, political parties and interest groups can ensure that these are accepted by the voters.

State bodies that make data available in the context of elections and votes meet the data protection transparency requirements by adhering in the performance of their tasks to the publicly accessible legal basis and any special provisions on the duty to provide information.

6.2 Proportionality

The principle of proportionality also applies 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.

6.3 Purpose limitation

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 for purposes other than those stated.

6.4 Data accuracy

Anyone in possession of a data file 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 is corrected or destroyed if, when taking account of the purpose for which it has been collected or processed, it is inaccurate or incomplete.

6.5 Data security

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 data controller who is required to protect personal data; every data processor must do so, even if the personal data concerned does not constitute a data file. 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 Breach of personality rights and grounds for justification

7.1 Breach of personality rights

Anyone who processes personal data as a private data controller may not unlawfully breach the personality rights of the data subject. A breach of personality rights occurs, for example, if a processing principle is violated (see Section 6), personal data is processed against the express will of the data subject or sensitive personal data or personal profiles are disclosed to third parties.

Example: A political party sends out a newsletter to subscribers. This data processing does not breach the personality rights of the subscribers. As soon as someone unsubscribes from the newsletter, if the party continues to send that person the newsletter, this would constitute a breach of their personality rights, as the data processing involved occurs against their express will.

Example: A lawyer runs for political office and sends election advertising to their client base. There is no congruent purpose between providing legal services and canvassing for election on one's own behalf. There is also no logical connection between the two activities. Furthermore, the clients' legitimate expectations do not involve a change in processing purpose. The lawyer may therefore not process the clients' contact data in a political context without first obtaining their consent.

A breach of personality rights is not unlawful if it is justified by the consent of the injured party, by an overriding private or public interest or by law. The statutory basis as grounds for justification will not be further discussed below (examples can be found in Section 4.3).

7.2 Overriding private or public interest

A breach of personality rights may be justified by overriding private or public interests. Whether the private or public interest prevails depends on the weighing of interests in the individual case. The seriousness of the breach of personality rights must be considered, as well as what the potential breach actually involves, and whether the private or public interest in processing the data is so significant that it appears objectively justified and reasonable that this should take precedence over the protection of the data subject's personality rights.

A legitimate private or even public interest can be claimed when processing data in a political context, and political rights are guaranteed by the Constitution. The extent to which this interest takes precedence over the protection of an individual's personality rights and is thus to be considered overriding depends in particular on which data is processed and how this is done.

Example: A political party purchases an address database originally collected for marketing purposes from an address dealer. It then uses these addresses to send out voting recommendations. Even though it may be assumed that the principle of purpose limitation is breached, the associated breach of personality rights is likely to be considered minor, so that it will ordinarily be justified by the overriding interest of the party.

7.3 Consent

If there is no overriding interest or if a data processor would not like to risk such an argument not holding up in a legal dispute, data processing that breaches the data subject's personality rights may only be justified with the active and informed consent of the data subject.

Consent is self-determined if the data subjects 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 they make their data available, but also as to what extent. 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 data subjects are given full and fair notice before registering that their data will be processed and of how the analysis methods used for this purpose function, including the use of automated programs and artificial intelligence. They must also be informed of their rights, such as the 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 how long data will be processed for and whether it may be passed on to third parties. The information begins on the registration page with a clearly visible summary of 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 ('social match').

7.4 Express consent

When sensitive personal data or personality profiles are processed, consent (self-determined and informed) must also be expressly given. The data subject must actively agree to their stored data being processed, for example by ticking a box on a website they have registered on. Declarations in which users accept conditions of use merely in a general manner do not constitute express consent. The same applies to declarations inviting users to subscribe to or comment on website content and the views presented, for example on social platforms. Moreover, a person may only give consent to their own data being used. Third parties must give their own consent to their data being processed.

8 Data processing in a political context

Data processing by private data controllers is permitted under Swiss law provided the personality rights of those involved are not breached. Personality rights may only be breached under circumstances in which this can be justified (see Section 7).
Legality must be ensured throughout the entire data processing process. To illustrate what this means in a political context, the process can be divided into four stages: data collection, data analysis, information targeting and addressing of data subjects.

8.1 Data collection

Where personal data is collected directly from the data subject, this must be done in such a way that the personality rights of the person are not violated (see also the explanations in Section 7 above). In this context, compliance with transparency and purpose limitation as well as the duty to provide information when obtaining sensitive personal data and when creating personality profiles is of central importance. Data subjects must therefore be informed in particular about what data is processed for what purposes and in what manner. After the new Federal Act on Data Protection comes into force in September 2023, the duty to provide information will also apply when collecting non-sensitive personal data (see the publication The new Data Protection Act from the FDPIC's perspective).

If the other processing principles are also complied with and neither sensitive personal data nor personality profiles are disclosed to third parties, the personality rights of the data subjects are not violated, so no particular grounds must be given for the data processing.

> *Example: A political party supplements the data collected from its newsletter mailing with information obtained by collecting signatures or by personally approaching the public at stalls, door-to-door canvassing or via telephone calls. Data is also obtained from publicly accessible sources such as telephone directories and public registers. The party obtains most of the data directly from the data subjects. When obtaining the data, it should inform the data subjects that it will use the data to contact them personally and possibly supplement it with other publicly available data.*

If it is unclear whether data processing breaches personality rights, it is recommended to obtain the consent of the data subjects, seeing as this is generally easily done in the circumstances described above.

As soon as personal data is collected from third parties, it is much more difficult to safeguard the personality rights of the data subjects. Particularly when data on a large number of data subjects is processed, it is unlikely that the principle of transparency can be complied with easily. Therefore, in such circumstances or if it is planned to disclose particularly sensitive personal data or personality profiles to third parties, justification should be provided for the breach of personality rights.

> *Example: A political interest group collects personal data from websites and internet portals with the help of web mining, commissions third parties to do so, or purchases such information. For this purpose web-crawler services are used, which systematically search the content of websites or for email addresses and collect the desired information. In this case, it is unlikely*

that the principle of transparency will be complied with, nor that data subjects are actively informed. The principle of purpose limitation could also be violated. There therefore should be an overriding interest in processing the data. If data collection involves a blatant violation of the law, as in the case of crawler services that ignore the terms of use of social networks, it can no longer be claimed that there is an overriding interest.

The same is true when data is collected with the help of campaign software. Designed more or less like a flexible content management system (CMS), such applications combine all common social networks into a system that allows interactions with specific groups of people. Once in possession of a person's email address, an interest group can use a specific function ('social match') to search for the person on social media and then add all the information found on this person to their data collection (see Section 7). Under certain circumstances, this data processing constitutes a serious breach of the data subject's personality rights, so that an overriding interest can no longer be claimed. In this case, the data subject's consent must be obtained.

8.2 Data analysis

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

Segmentation based on individuals' demographic, ideological, socioeconomic and psychological characteristics, as well as various artificial intelligence methods, is used to predict their behaviour. The resulting profiles can be used to target the data subjects with political messages.

When compiling data, the controllers of the data file must be aware that a large amount of sensitive or intrinsically non-sensitive data taken together can form a personality profile within the meaning of the Data Protection Act. Such profiles are subject to qualified or stricter legal protection. The Federal Administrative Court commented in detail on this issue in the Moneyhouse ruling (Section 5). Qualified protection also applies to the processing of sensitive data such as ideological or political views, to which the law gives special protection (Section 5.2).

As far as it is known, there is no statutory basis that allows a public body to carry out political analyses on the basis of personal data.

8.3 Information targeting

Based on the assumption that people in a common profile group react particularly strongly to certain messages, political parties and interest groups aim to target information at individual groups via email distribution lists or social media and so seek to influence political opinion in the run-up to votes and elections. In so-called 'microtargeting', both the content of messages and 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 the targets' preferred communication channels. Microtargeting can be particularly effective in popular votes, where experience shows that large numbers of potential voters often do not have a firm opinion on the particular issues.

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 persons to vote or to discourage them from doing

so, depending on whether the evaluated data identify the data subject as a political friend or opponent. A further possibility is simply to encourage people to vote, but to send out these messages selectively – i.e. not to suspected political opponents.

8.4 Addressing of data subjects

Frequently, data subjects first become aware that their data has been processed when they receive a political message (see Sections 8.1–8.3). This is particularly the case if the processing is based on an overriding interest. For this reason, the data subjects must receive the information at the same time as the political message is sent. They must be informed who is responsible for the message received, where further information on the associated data processing can be obtained and how they can claim their rights as data subjects. They should be informed as clearly as possible about the data processing that has taken place (see Sections 8.1–8.3) so that the context of the political message can be understood. They must also have a quick and easy option to say that they do not wish to receive the data.

8.5 Consent

For the discussion on consent, see Sections 7.3 and 7.4 above.

8.6 Rights of data subjects

The data file controllers are required to ensure that the rights of the data subjects are protected. For example, all data subjects have the right to request information from the data file controller about the data processed on them, to correct incorrect personal data and to have data deleted.
Therefore, all data subjects must be able to exercise their right to information, correction and deletion in an appropriate manner. This starts with informing them about their rights and how and where they can claim them. To ensure this, data file controllers can provide information on their website or address the data subjects directly. If data processing is carried out by joint controllers or if third parties process the data, it must be easy for the data subjects to identify against whom they can claim their rights.

Data subjects must be able to exercise their rights easily and generally without incurring costs.

9 Requirements for websites

Where personal data on a website is processed, data protection processing principles must be observed. Public bodies are also bound by this legal requirement. The following questions provide a check of whether these principles are observed:

- Are website visitors informed in a clear, easily accessible manner and in comprehensible language about the various tools used and the purpose of data collection (see Section 6.1)?
- Is there a multi-level information system for people who need more detailed information, i.e. are there more detailed technical explanations in addition to easily understandable, concise ones?
- Can visitors individually (‘granularly’) choose whether or which of the web-tracking tools they want to use?

- When social plug-ins or similar services are used to link to Facebook, are technologies used that ensure that tracking or data transfer only occurs once the user's consent has been given (see Sections 7.3 and 7.4)?

- Are data subjects informed about their rights, in particular their right to information? Are the necessary technological and organisational measures in place so that information can be provided (see Section 8.6)?

- Does the tracking process only collect data that is necessary for the intended use (See Sections 6.1 and 6.3)?

- Have solutions been selected for web-tracking and web-analysis that do not permit third parties to use data for their own purposes, e.g. the use of analytical tools that the data controller has installed themselves or that shorten the IP address (see Section 6.3)?

- If third parties have been commissioned to process the data, are the data subjects informed about this? Are the third-party data processors required to prove that they have taken organisational and technical measures to ensure data security and are these monitored (see Sections 4.2 and 6.5)?

- Is the method of data transfer (e.g. contact form) encrypted?

- Are the data subjects informed in advance about any further use of their email addresses, e.g. for 'social matching', and has separate consent been obtained for this (see Sections 6.1, 7.3 and 7.4)?

10 Practical examples

Example 1

A political party attempts to recruit members at events and on its website. It offers these potential members the opportunity to subscribe to its newsletter by providing their email address. The party intends to make all the email addresses obtained in this way available to the operators of a social media company and thus use the company's targeting and propagation techniques to address its political advertising specifically to people with similar personality profiles.

There is no obvious logical connection between the purpose of providing the website visitors with general news about the party and the additional purpose of sending out targeted political messages with ideological aspects aimed at specific personality profiles. The additional purpose thus does not meet the legitimate expectations of the newsletter recipients. The party cannot claim sufficient overriding private and public interests that could justify the breach of personality rights.

It may not therefore use the email addresses without informing the recipients in advance and gaining their express consent to the use of their data for targeted and personalised political advertising.

Example 2

An advertising agency working for a political party offers a job aptitude test via social media that includes a psychological evaluation.

The completed test gives the social media operators information about the test-taker's education, occupation, employment status, age, hobbies, and email address and contacts. The advertising agency buys this information from the social media operators so that it can target its client’s political advertising at the most appropriate addressees.

The use of such targeting techniques violates the principles of purpose limitation and processing in good faith. Since the data processor cannot claim an overriding private or public interest, before the requested data is collected, the test-takers must be informed that it will also be processed for the purpose of targeted political marketing and so they must expressly consent to this additional processing.

11 Summary overview

A **Parties and interest groups**	Where a party or lobby group is the ***controller of a data file*** (Sections 4.1 and 4.2), it 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 (Section 6). • ***Authorised third parties*** **acting as joint controllers** are required to provide evidence that they meet all legal requirements on data protection (Section 6). • ***Authorised third parties*** acting as data processors are contractually obliged to meet all legal requirements on data protection, and in particular to provide evidence that they are taking appropriate organisational and technical data security measures (Section 6.5) and that they process personal data only for contractually agreed purposes. • The right of voters to ***transparency*** (Sections 6.1 and 9) is met by ***information published on the website*** on - the identity of the data controllers; - the categories of data processed; - the collection of data from third-party sources; - the current purpose of processing and, where necessary, the reason for processing; - the processing methods, 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 applicable terms of use of third parties and their sources. • Processing takes place in compliance with the principles of ***purpose limitation*** (Section 6.3) and ***proportionality*** (Section 6.2), according to which any further processing must always be for the purpose underlying the data collection and must cease when this purpose is achieved; • Any ***consent*** required for processing personal data in the context of the political process is expressly obtained (Section 7.4); • The ***accuracy of the data*** is guaranteed even if third parties are involved and data that is no longer required is deleted (Section 6.4); • The data protection, ***organisational and technical risks are assessed*** and appropriate protective measures taken (Section 6); • Internal ***documentation*** exists showing how the security of the various categories of processed data is guaranteed (Section 6); • When using the services or applications of third parties (e.g. newsletter services or the planning and administration of door-to-door canvassing), the requirements on disclosing data to

	third parties and on transferring personal data abroad must be observed. See the information on this on the FDPIC website (link: Transborder data flows (admin.ch)) and the following documents as a minimum: - Position paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 para. 1 FADP (Link: position paper) - Guide to assessing permissibility of data transfers abroad (Link: PDF guide) • The data subjects' ***right 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 **Voting rights registers**	Authorities responsible for maintaining the **residents' register and electoral roll** (Section 4.3) must ensure that • data processing does not exceed the ***legal requirements*** with regard to purpose, content, scope and duration; • personal data is only passed on where there is a sufficient legal basis for doing so, or the data has been effectively pseudonymised in advance; • where this is not anyway excluded by law, ***citizens can refuse*** to have their data passed on for the purposes of political advertising; • the ***risks*** to technical and organisational security are ***assessed and documented***, including re-identification risks, and the necessary protective measures are taken (Section 6.5); • 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 4.5) or data analysis companies (Section 4.4) process data in the context of the political process as the ***controller*** with overall responsibility, they must take account of the information in Table A. Where they act as ***processors*** and process data in the context of the political process: • they must adhere to the obligations agreed by contract with the data controller; • before concluding a contract, they must make sure that their client is willing and technically and organisationally able to process the data received in accordance with the law and the contract; • they must comply with the rules in the Moneyhouse decision on combining data from different sources to create profiles (Section 5); • they must ensure data security by assessing and documenting risks and taking the necessary protective measures (Section 6.5); • if so requested, they must help their clients to conduct 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 transferred data; • whether and, if so, for what purposes and in what form the data subjects were able to consent to the data being transferred and processed.
D **Data platforms**	Irrespective of whether private data platforms (Section 4.6) process information in the context of the political process as the controller or as the processor, processing is generally governed by ***general terms and conditions of business and use***. • They must respect the right of voters to ***transparent data processing*** (Sections 6.1 and 8.4) 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 ***controller***, they must also comply with the rules in Table A. Where they process data as a ***third-party processor***, 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 personality 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 dealers, data analysis companies or data platforms, private individuals must obtain the ***express prior consent*** of the data subjects. They must ensure that any software that accesses this data comes from a reliable source.