Personal data protection and digital security

Personal data protection

Privacy policy is a document that needs to be created with a goal of providing information to the public about why and in what way the operator uses and processes the personal data of those people.

The duty to inform comes from the legal obligation of the operator[1] to provide legally prescribed information in advance to people whose data is being collected. In order for the requested information to be available to interested persons in advance, the standard practice is that the privacy policy is publicly published on the operator's website.

The text below is an example of a form with which the operator can describe the processing of personal data they collect through their website within the privacy policy. The headlines of this example follow the mandatory information which the operator is obliged to provide according to the Law on Protection of Personal Data and other applicable regulations.

There are explanations in the footnotes for how to adapt this example for the needs of a specific operator. In this sense, it is necessary to enter information that is relevant to the specific operator within each point (headline), including information that some things are not processed. After finalizing the text with the necessary information, the footnotes should be deleted.

If the operator does not collect personal data, it is recommended to publish a notice stating this on the website.

An example of a specific privacy policy that was developed in accordance with these recommendations, which was developed by SHARE Foundation from Serbia, can be found here.

Download the privacy policy document in a Word document.

[1] Any public body, physical or legal person, agency or other body that independently or together with others conducts, processes and determines the purpose and method of processing personal data based on laws or regulations.

Privacy Policy

In the following text, you can inform yourself about in which situations, for what purposes and in what way the operator listed below processes personal data, taking into account the information that the operators are obliged to present according to the provisions of the Law.[2]

1) Identity and contact details of the operator

<Name>
<Address>
<City, Country>

2) Contact details of the operator in regards to the protection of personal data

<provide contact details>

3) Purpose of processing, source of data and legal basis for processing[3]

Purpouse[4]	***Type***[5] ***and source of data***[6]	***Legal basis***[7]
<state the purpose of data processing>	<specify the ways of collection and sources of data for this purpose>	<specify the legal basis for data processing for this purpose>
<state the purpose of data processing>	<specify the ways of collection and sources of data for this purpose>	<specify the legal basis for data processing for this purpose>

[2] The template presented in this chapter should be coordinated with the exact personal data that the organization working on the establishment of privacy policies is obliged to present, in accordance with the Law on the Protection of Personal Data of that country.

[3] The information under this headline can be provided in a form of text or a table. In the final document, it is necessary to delete the table, i.e. the narrative text, depending on which of the two forms is the information given under this title.

[4] The purpose can be, for example: commenting on the website; filling out the contact form on the website; participation in surveys; subscription to the newsletter; registration on the website; donating to the operator, etc.

[5] Data types can be, for example: name; e-mail address; telephone; IP address; content of a comment or message; bank account number, etc.

[6] Data can be collected directly from the person who provides it to the operator - for example by the person just entering it on the site, or indirectly - for example, from publicly available sources.

[7] The legal basis for processing can be consent of the person, the legitimate interest of the operator, a contract that the operator has with the person or fulfillment of legal obligations of the operator. If you are not sure, you should consult a lawyer regarding the appropriate legal basis.

or

<in the form of a narrative text, state / describe separately each purpose, information on how the data was collected to fulfill that purpose and, if necessary, what data it is, as well as what is the legal basis for each purpose>

4) Recipients of personal data[8]

The operator shares personal data with <specify data recipients, i.e. organizations with which data is shared>.

5) Transfer of personal data to another country[9]

Personal data is processed in <specify country where data is stored / hosted>.

6) The retention period of personal data, i.e. criteria for its determination[10]

<specify the data retention period, i.e. the moment after which the data is deleted, and if there are multiple purposes, it is necessary to specify different deadlines for each of the processing purposes>.

7) The rights of persons to whom the data refers

Any person to whom the data we process refers to, has the right to request from the operator:

- to inform them truthfully and completely about the processing of their data;
- the right to access and/or a copy of the data refering to them;
- the right to correct and add incorrect or incomplete data, at any time;
- the right to erasure, which can be granted in accordance with legal conditions, i.e. when: personal data is no longer necessary to achieve the purpose for which it was collected or processed in other ways; the person to whom the data refers to has filed an objection to the processing based on the legitimate interest of the operator, and there is no other legal basis for

---

[8] Enter the recipients of the data, with whom the operator shares the data (for the sake of understanding, it is recommended to specify the reason for which the data is shared). These can be business associates, related business companies or organizations, courier services, legal and financial consultants, competent state authorities, etc. If there are no recipients with whom personal data is shared, it should be written in this headline.

[9] Enter information about which countries the data is processed in. If necessary, check where the website is hosted. If the data is processed in countries that are not considered adequate according to the relevant regulations, state the legal basis for the transfer of data to inadequate countries.

For example: *Personal data is processed in Serbia and India. The transfer of data to India, which is not considered a country that provides an adequate level of data protection, is regulated and secured by Standard Contractual Clauses.*

[10] Examples of the retention period can be: the personal data you provide when leaving a comment is stored permanently, i.e. they are not deleted like the comments themselves; the e-mail you provided in order to receive the newsletter is deleted when you unsubscribe; the data you provide in the contact form on the website is stored for a maximum of one year after sending the message.

- the processing; personal data was illegally processed; personal data must be deleted in order to fulfill the legal obligations of the operator;
- the right to limit processing, which can be complied with if the required conditions are met: if the person to whom the data refers has contested the accuracy of the personal data, and the operator needs time that allows him to check the accuracy; if the processing is illegal, and the person objects to the deletion and instead of the deletion requests the restriction of use of the data; the operator no longer needs the personal data to achieve the purpose of processing, but the person requested it for the purpose of submitting, realizing or defending a legal claim; or the person has already filed an objection to the processing, and an assessment is underway as to whether the legal basis for the processing by the operator outweighs the interests of the person;
- data transfer in machine-readable form, which exists in cases where it is applicable, i.e. if it is technically possible because the data is machine-readable and when the legal basis for processing is the consent of the person or a contractual relationship with the person to whom the data refers.
- the right to withdraw their consent to the processing of certain data at any time, if the consent is a legal basis for the processing.

The person also has the right to object, if the person to whom the data refers to considers that the legitimate interest of the operator on the basis of which the data is processed is not justified, that is, that it threatens the rights, freedom and interests of that person.

In case of automated processing of personal data and decision-making, the person has the right to human intervention, as well as the right to express their opinion on the decision or challenge the decision.

8) The right to file a complaint

The person has the right to file a complaint against the operator's actions to the competent authority in accordance with the law of the country in which the operator operates.

9) Existence of automated decision-making, including profiling[11]

The operator does not perform automated decision-making, nor profiling, based on personal data.

10) Cookie Policy[12]

[11] The media usually do not perform profiling (creation of unique profiles) and automated decision-making about rights and interests of visitors to their websites (making decisions without human intervention, but only through "algorithms"). If the operator still does this, it is necessary to clearly and comprehensibly explain the purposes and ways in which such processing is carried out.

[12] If you use cookies that can lead to the direct or indirect identification of certain users of your website (through any unique identifier), the use of such cookies is also considered as processing of personal data.
In that case, you need to first determine if there are any cookies that you have a legitimate interest in using (such as strictly necessary cookies), which in that case is a legal basis for data processing.
All other cookies can only be used based on the consent of the website visitor.
Therefore, it is then necessary and recommended that you enable a pop-up option in which website visitors would

<In this headline, only an example is given of how the operator can describe the use of cookies on their website. If you want to use the text below, it needs to be adapted to the specific web page>.

A "cookie" is a small piece of data that a website can send to your browser, which can then be stored on your hard drive. If you are concerned about your privacy and the use of "cookie" technology, you can set your browser to notify you when you receive a "cookie". Cookies can help you be more efficient and benefit from «memory» functions, for example when a website remembers your language in which you viewed the page from a previous visit. Cookies allow you to save your preferences, to save products and services and to customize pages.

The operator uses cookies on their site in order to provide services and functionality to their users. You can restrict or disable the use of cookies through your internet browser, but without cookies you will not be able to use all the functionalities of the site.

There are different types of cookies, and according to the criteria of who places cookies on the website, we distinguish:

- first party cookies – cookies set by the operator when you use the website, and
- third party cookies – cookies set by another organization when you use the website (some websites may also contain content from other sites that may set their own cookies).

Regarding the purpose, we use the following types of cookies on the site:

- Strictly Necessary Cookies – These cookies are necessary to manage your connection status.
- Functional cookies - these cookies allow the website to remember your previous actions in order to provide you with advanced functionality.
- Analytical cookies - these cookies allow us to collect data about your use of the website in order to improve its performance and design. To disable Google Analytics cookies, download and install this plugin.
- Marketing cookies - these cookies are used to collect various information about your visit to our site, such as information about the content you have viewed, the links you have followed, your browser, device or IP address.

---

have the option to refuse all cookies that cannot be justified by legitimate interest, such as analytical, marketing and third-party cookies.

Digital security

Internal security policies

Digital security is of key importance for media organizations and individuals who make them, that is, journalists and other employees, as well as sources with which journalists come into contact during research. In order to make the use of technology during their work safer, the media should adopt appropriate policies and procedures that will help them in that. In the event of technical incidents, such as an attack on a media website or account takeover, these policies can help prevent or at least minimize damage to an organization's resources.

Depending on the capacity and resources of the organization, the creation of internal security policies involves the participation of management, editorial staff, team members in charge of IT, as well as journalists and other employees who possess more advanced technical skills that they can pass on to others. Training and education of employees is important in order to apply procedures and policies without disrupting regular work processes.

Every internal document in the field of digital security should be adapted to the real needs and capabilities of the organization, to be precise and understandable to all interested parties. Internal policies must be available in electronic form only to team members, so not to the public. For these purposes, a platform for internal communication such as Mattermost, Rocket.Chat, Element can be used so that employees, in case of doubts or working outside the premises of the organization, can have access to documentation and consult with colleagues or persons responsible for monitoring the application of policies, e.g. editors.

Examples of internal documents are password policy, the policy for use of official e-mail addresses and accompanying accounts, as well as the security plan.

Policy of passwords

The goal of the document below is to help organizations create a unique policy for use and management of passwords, in order to provide clear procedures. The password policy enables the organization and its members to safely create, use, store and modify passwords, which represent the basic authentication mechanism, i.e. protection of organizational resources from unauthorized access.

_____ (Name of organization)

1. This policy applies to passwords used to protect accounts, devices, documents, databases, and other resources managed by _____ (Name of organization).

2. A single password must not be used to protect multiple different resources. Passwords must not be publicly displayed or shared with unauthorized persons.

3. If there is a technical possibility, it is necessary to introduce double verification (2-step verification) on each resource managed by _____ (Name of organization).

4. Changing of all passwords for resources managed by _____ (Name of organization) is done for a period of _____ months.

5. Passwords must be at least 15 characters long, must contain special characters (e.g. punctuation marks), uppercase letters, lowercase letters and numbers. Passwords must not contain personal data of employees (e.g. first names, surnames, dates of birth, phone numbers, residential addresses) or persons close to them (e.g. immediate family members).

6. For particularly sensitive resources (e.g. databases containing data of a particularly sensitive nature: victims of violence, health status, sexual orientation, etc.) it is necessary to introduce protective phrases (passphrases) consisting of strings of randomly selected words in combination with other mandatory elements for passwords from point 5 of this policy. Security phrases must be at least 20 characters long.

7. The person in the organization responsible for administering passwords is _____ (name and surname, workplace).

8. Upon assigning a password for accounts used for the work and activities of _____ (Name of organization), such as official e-mail accounts, employees are required to change the given password in accordance with this policy immediately after receiving it from the competent person who created the account (e.g. technical administrator) and assigned it to the employee. New passwords must be generated and stored in a password manager.

9. Passwords and security phrases are stored in special applications intended exclusively for password management (e.g. KeePass, KeePassXC) that store the password base on the device's local memory. Saving passwords in internet browsers and on online password saving sites is not allowed.

10. Making a backup copy of the password database stored on an external memory (e.g. external hard drive, USB) is done every time passwords and security phrases are changed (adding new ones or changing old ones) and the date when it was created must be indicated in the file name.

11. In the event that an employee notices or suspects that any resource managed by _____ (Name of organization) has been compromised, they will immediately inform their supervisor and change the password or security phrase for that resource, and if it is a shared resource, they will notify the person in the organization in charge of password administration.

12. This policy is coming into force ____ days after its adoption.

Date:_____ Authorized person of the organization:_____
Place:_____

Policy on the use of e-mail and accompanying accounts

Using the document below, organizations can create a unique policy for the use and management of official e-mail accounts and related accounts (i.e. complete productivity service packages offered by providers such as Google or Microsoft) so that it is clear for what purposes they can be used, to whom they are assigned, how to act during the departure of team members from the organization and similar. The account policy enables organizations and their members to manage organization-owned accounts in ways that reduce potential risks within digital security and use them in accordance with prescribed purposes.

Name and address of the organization

E-mail and follow-up account usage policy _____ (Name of organization)

This policy contains the conditions for using e-mail and accompanying accounts on internet domains owned by _____, namely: _____ (enter domains, e.g. organizacija.rs) (in the following text: domains _____).

1. E-mail and accompanying accounts created for the purposes of work, practice and volunteering in _____ are owned by _____.
2. _____ manages accounts and issues them for use to persons who are employed in _____, persons who are on praxis and persons who volunteer.
3. The person to whom the e-mail account was issued uses the account and _____ has no insight into the content of that account or its supporting parts (cloud storage, collaborative documents, etc.).
4. Accounts on domains _____ are used exclusively for the purposes specified by _____.
5. In case of termination of the relationship between _____ and the person to whom the account was issued, ownership of the account remains with _____.
6. _____ will leave a period of 30 days from the date of termination of the relationship, for the person to whom the account was issued to collect all content from the account that they think they will need.
7. After the expiration of 30 days from the termination of the relationship, the account will be deleted, and a copy of the content will be archived for the purposes of _____.
8. The policy comes into force on the date of adoption.
9. Persons to whom accounts have been assigned will be notified of any future changes to this policy.

Place and date, Responsible person

_____

Security plan

The security plan aims to help organizations create preventive and reactive measures regarding technical incidents, consider possible risks and threats to the organization's technical infrastructure, prescribe procedures and steps in case of dealing with different types of technical incidents, etc. While it's not possible to predict every single technical attack scenario, having a security plan can prevent or minimize damage and to help in recovery.

When creating a security plan, consider the following:

Goals: set a realistic primary goal or several secondary goals, so that the prescribed measures are actually applied to achieve the given goals.

Threats and risks: think about possible scenarios of threats to the digital security of your organization and its members, this will help you to identify possible threats and risks to digital security more precisely and prepare better to deal with them.

Preventive steps: list realistic steps you can take when it comes to protection of digital security, taking into account the threats, risks and capacities of the organization itself (technical, organizational and personnel).

Steps in the event of an incident: consider possible incident scenarios (e.g. unauthorized takeover of social media accounts) and define the necessary steps in given situations. While it's not realistic to predict all scenarios, choose a few that you think are most realistic to happen or that have already happened to your organization.

Recommended devices and equipment: Create a list of hardware and software solutions that have good reputation and reviews and are recommended by the expert community. Keep in mind the capacities of the organization, and if you are not sure what would best suit your needs, seek external advice.

Application of internal procedures: Specifically describe the application of your security procedures to several examples of incidents that you believe are most realistic to happen or that you have previously experienced in the organization.

Security plan

GOAL	**Improve the digital security of the organization as a whole and its individual members**
THREATS AND RISKS	• Compromisation of personal data and confidential information (documents, correspondence…) • Compromisation of the organization's technical infrastructure and resources • Loss of control over infrastructure and data as a result
PREVENTIVE STEPS	• Access to the infrastructure and resources of the organization (servers, network equipment, accounts on social networks, admin panels of websites, etc.) enabled only to certain persons and protected by strong passwords stored in special applications for that purpose (password managers, e.g. KeePass) • Adopted organization password policy • Double authentication (2-step authentication) included on all user accounts that support it. • Keep especially sensitive data (e.g. information about victims of sexual violence) encrypted, on special devices that are not used for daily work. • Employee devices protected by passwords/pin codes • Regular backup of data on local devices (e.g. external hard drives) and/or online (on the organization's server or on cloud services, e.g. Dropbox, Google Drive, OneDrive...). **However, particularly sensitive personal data and other confidential information should not be stored on cloud services.** • Use encrypted e-mails (PGP) and chat applications (Signal) to exchange confidential information.

STEPS IN THE EVENT OF AN INCIDENT	• Notify competent colleagues (administrators in charge of technical infrastructure in the organization) and technical support (e.g. hosting company) as soon as possible and follow their instructions • Collect all available information about the incident (time, place, activities during the incident, IP addresses, logs, screenshots, last correct configurations...) in order to determine the damage and consequences • Notify special/sectoral cyber incident response teams, such as the National CERT (Computer Emergency Response Team) • Report the incident to the competent state authorities • Check the last available version of data/system configuration to attempt to return to the previous state and reconstruct
RECOMMENDED DEVICES AND EQUIPMENT	• Mobile phones with installed encrypted chat applications (Signal) • Computers: installed and regularly updated anti-virus software, as well as all other software used • Computers: Password manager installed (e.g. KeePass, KeePassXC) • Computers: installed hard drive encryption software (VeraCrypt) • Created PGP keys for employee e-mails and installed appropriate software (e.g. Thunderbird, Gpg4Win, Mailvelope) • Browsers: Mozilla Firefox, installed plug-ins (HTTPS Everywhere, Privacy Badger, uBlock Origin, minerBlock, Facebook Container) or Brave on which Google Chrome plug-in versions can be installed • A reliable VPN (e.g. Mullvad, ProtonVPN) and Tor Browser installed on devices

APPLICATION OF INTERNAL PROCEDURES (EXAMPLE)	It has been noticed among employees that the organization's website is unavailable or has difficulty loading 1. Check the availability of the page on the "Down For Everyone Or Just Me" service (https://downforeveryoneorjustme.com/) and internet connection 2. Scan all computers and devices with an anti-virus software 3. If it is determined that it is not a technical problem, the employee informs the technical administrator of the organization personally or via a secure communication channel (Signal chat, encrypted e-mail message). 4. The administrator, in cooperation with technical support, performs an infrastructure check and if it is determined that there has been unusual traffic, unauthorized access or other violations of the integrity of the information system, collects digital evidence 5. Next is an attempt to restore data/restore functionality using backups and/or last good configurations 6. After that is determination of the type of attack and legal qualifications, notification of competent authorities and preparation of submissions (e.g. criminal charges) in cooperation with special/sectoral teams