INIMÕIGUSTE KESKUS

Privacy and data protection

Every click counts, reading your data amongst other things!

When navigating online, making purchases, or communicating, you constantly leave behind **digital footprints** which may have very real consequences to your privacy and other rights. However, it often remains unclear to us to which extent our personal information is actually used and shared.

You need to be aware of your personal information. In today's data society it is increasingly important to know who is processing your data, along with how and why such information is being processed. You have the right to be notified of any processing of your personal data, even in a situation in which different authorities or individuals are making use of your data to direct you via advertising media or other media content which may be found in social media sources. For example, have you noticed that if you are looking for entertainment events or a new piece of furniture, you will suddenly start to see related adverts when surfing online? Many companies collect and share information about you which allows them to predict your behaviour. Then they are able to send you targeted and personalised content which is customised to your behaviour and interests. This is referred to as **microtargeting**. On the one hand, this may seem convenient and appealing because you are being offered precisely the sort of content you want to see but, on the other hand you may lose your priceless privacy and even more. Social media platforms have created what has been termed psychological profiles so that they can effectively **profile** the content being displayed, going as far as assessing the openness of people to new experiences, especially in terms of their determination or extraversion, their preparedness for cooperation, or their potential levels of neuroticism. Such in-depth data can be used to successfully persuade users to buy, click, or choose.

In addition to the fact that you may find yourself entertaining yourself online without giving it a second thought, or perhaps making unplanned purchases, the data economy may also place **democracy** at risk. Did you know that the same methods have been used by the organisers of political campaigns in order to customise the campaign message for specific voters in order to sway their vote?

As an example, this model has been used by Cambridge Analytica in Trump's election campaign and also before the Brexit vote. Those processes involved buying targeted advertising which was placed online, taking into consideration the preferences and expectations of certain user groups on Facebook.

Furthermore, if people only see news features which match their personal views, society may end up fractured. Personalised news sources tend to influence people to behave in a certain manner, which may result in important decisions being skewed from a national perspective.

Amongst other things, cookies on computers are used for data collection purposes.

Cookies (online trackers)

Microtargeting works by using electronic means, such as cookies, plug-ins, or tracking pixels. Such tools make it possible to monitor your online traffic, whether this involves your habits, likes, or social connections, all for the purposes of profiling you.

Cookies involve information which is used by websites in order to preserve settings and details regarding visits to the website. There are different types of cookie, some of which are certainly necessary while others breach your privacy. Some cookies are created to manage websites, others are created for the personalisation of websites or even for the monitoring and identification of users. So, as can be seen, cookies are used to obtain further information about you.

Cookies can be managed by working through the privacy settings of internet browsers. Browser extensions may also be used. These help to restrict the tracking of your internet traffic. In order to restrict microtargeting, check your account and social media settings.

Your browser history, cookies, and temporary internet files are not saved when you are browsing in incognito or privacy modes, but you should still keep in mind the fact that third parties may eavesdrop on your online traffic and monitor users of the incognito mode.

For advice about data protection, please send us an email containing your questions or problems via the following address:

info@humanrights.ee

Data leaks and cyber-operations

In addition to data collection which takes place through various means such as, for example, the use of cookies, an increasing number of cyber-attacks are being targeted against internet users in order to obtain our personal information, while additionally attempting to infect our computers with malware, or to gain access to company systems thanks to the potential carelessness of an employee. To ensure proper and stringent data protection, it is important to practice a modern cyber-hygiene regime and to apply proper data protection principles. Read more in the chapter on cyber-hygiene.

You have the right to be aware about who is directing you and how your data could be used.

1. Privacy and data protection

What is privacy?

The right to privacy helps to protect both your personal and family life, along with ensuring the inviolability of the home, and the privacy of communications. Privacy is also part of an individual's general right to free self-determination, which refers to the individual's right to decide and determine who that individual may be, and what impression is left of them. All individuals have the right to decide whether - and to what extent - they share their private lives with other people, companies, the public, or the state. The right

to self-determination regarding one's information is especially endangered in today's ever-broadening data society in which the systems which are used by internet platforms constantly customise our online environments and predict our behaviour, preferences, and vulnerability. At the same time, we have the right to privacy online, as well as offline.

Privacy is not a privilege, or a benefit which is only available to a few selected individuals, or something which is only sought out by famous people.

Privacy is the right of **each and every individual**. Everyone has the right to free self-determination and to their personal choices being respected by other people, companies, and the state.

Privacy supports the protection of other human rights.

The right to privacy **protects** the physical and mental integrity of an individual, ensuring their moral and intellectual freedom, their reputation and honour. The right to privacy protects a person's name and identity from unlawful use and their information from being disclosed. For example, an individual has the right to decide whether photos and videos of them may be shared publicly, along with which photos and videos are shared of them. Identity theft, for example by creating fake accounts, is also prohibited.

The right to privacy also protects people from unauthorised spying, monitoring, or harassment. The right to privacy additionally extends to an individual's **work life**. For example, it is not permitted to install cameras in employee locker rooms without a valid reason, or to conduct unauthorised searches in a solicitor's office, or to disclose information about an employee's health. The right to privacy protects a person's family life and is therefore related to the right to get married and start a family (Article 12 of the 'Universal Declaration of Human Rights'). While Article 12 protects the right to get married, Article 8 protects the right to get a divorce. The right to privacy also extends to the protection of family life, protecting the right to communicate with one's child. Furthermore, the right to privacy protects the right to choose one's social connections or voluntary sexual contacts, as well as one's sexual identity. The criminalisation of homosexuality, the prohibition of name changes or gender reassignment, or placing restrictions upon choosing a child's name without a valid reason are also deemed to be violations of privacy, with these just being a few examples.

The right to privacy also extends to **communications privacy**. Any violation of one's communications privacy is only permitted in limited cases and if there is a specific reason. Private and arbitrary spying, searches without a clearly defined or legal basis, secret wire-tapping, interfering with calls or data connections, and recording conversations are all prohibited. Any searches which are conducted by the police must be clearly defined, while also observing human dignity, and only being permitted to the extent which is required to be able to achieve a specific purpose. Neither blanket surveillance of the population or the blanket retention of communications data is permitted (even for the purposes of investigating serious crimes). The state must very clearly specify in

legislation those cases in which it is permitted to use surveillance and how it may treat any data which may be collected in the future.

In addition to the state's obligation to refrain from arbitrary interference with individual privacies, the state must also ensure efficient protection of the private and family lives of its citizens, while also undertaking measures to ensure that protection, including within the area of relationships between people or with mass media outlets. The state must also protect its citizens from companies or organisations which use any form of technology or business models which violate the rights of individuals.

In which cases is it permitted to interfere within an individual's private sphere?

Article 8 of the European Conventions on Human Rights states:

> **'Everyone has the right to respect for their private and family life, their home and their correspondence'**

No one may unlawfully interfere with the private sphere of an individual or disgrace the honour or good name of an individual. An individual's privacy may only be interfered with if such interference is compliant with the law and in addition is required in a democratic society in the interests of national security, public security, or the economic welfare of the state, or to prevent lawlessness or a crime, or to protect the health of individuals, or the morality or rights and freedoms of other people.

The right to interfere with someone's personal sphere may arise from the 'Criminal Procedure Code', for example. In this area, if an individual has committed a crime then an investigative body may search their home or make enquiries of data processors, such as banks, once they have acquired the relevant permit. Such enquiries and searches must clearly be defined and the police may not arbitrarily investigate an individual's private sphere. Mass surveillance of citizens by the state is not even permitted for the purposes of combating serious crime or terrorism, as this would disproportionately violate the rights of individuals to privacy.

The following pieces of legislation protect the private lives of individuals:

- at the domestic level, through the national constitution (§ 26) and in national courts;
- at the international level, through the UN's Universal Declaration of Human Rights (Article 12) and the International Court of Justice;

- through the European Convention on Human Rights (Article 8) and the European Court of Human Rights;
- and also through the Charter of Fundamental Rights of the European Union (Article 7) and the European Court of Justice

What is data protection?

Anyone is entitled to knowing that their personal data is being protected. The right to data protection is closely related to the right to privacy, something which has become especially topical in connection with technological development. From the perspective of data protection, those parts of privacy are especially important where they allow for the **identification** of an individual and where they are used by an individual to determine themselves in their communications with other people and/or the state. Therefore the very identity of an individual is the main cornerstone of privacy. Identity is what differentiates one person from everyone else, such as a person's name, or an identification number (such as a personal identification code) which has been issued by the state in those countries which have personal ID cards, or their ethnic origin, appearance, character, behaviour, personal space, or social network, and so on. Personal information also includes an individual's personal email address(es), credit card details, communications or location records, receipts for possible social assistance, or network identifiers (such as an IP address or cookies). Therefore any information which makes it possible to identify an individual is included Under the umbrella of **personal data**.

Special types of personal data can include such personal information which calls for special protection, as any leaks of such information can result in an even greater threat to an individual's privacy. Special types of personal data can include information which could reveal someone's racial or ethnic origin, their political opinions, religious or philosophical beliefs, trade union membership, biometric data which is used for the unique identification of a private individual (a so-called 'natural person' in law) (whether DNA, facial geometry, voice recordings, fingerprints, palm prints, and iris images), information about their health, or information on their sex life and sexual orientation.

London and China, for example, widely use **facial recognition technology** (which includes the widespread use of closed circuit cameras), with that technology processing special types of personal information. Such technology may also be used for the purposes of discrimination or to restrict the rights of citizens, in addition to maintaining public order. Such forms of technology also violates the right of the individuals to be able to maintain their privacy.

Leaks of personal data may result in a risk to an individual's life or health, identity theft, discrimination, or financial or reputation-based damage, in addition to loss of

Anyone is entitled to the protection of their personal data

privacy. Therefore privacy protects everyone's freedom to enjoy other human rights.

Article 8 of the European Union's 'Charter of Fundamental Rights' states the following: '**Anyone is entitled to the protection of their personal data**. Such data must be processed **fairly** for specified **purposes**, and on the basis of the provision of **consent** by the person concerned, or some other legitimate basis which is laid down by law. Everyone has the right to **access data which has been collected where such data may relate to the individual concerned, along with the right to have such data corrected**. Compliance with these rules is subject to checks and controls by an independent authority'.

Specific data protection-related rights and obligations are laid down by special regulations, such as the directly-applicable 'General Data Protection Regulation' (GDPR), as well as the national 'Personal Data Protection Act'.

The GDPR establishes the general principles of data processing: such processing must be legal, fair, and transparent, as well as purposeful; as little data as possible may be collected, used, and retained, and the data may only be retained for as long as necessary; the accuracy and precision of the data must be ensured, along with the security (in terms of accessibility, integrity, and confidentiality), and liability.

There must be a legal basis for any data processing. Your **consent** is one of those legal bases. Consent to the processing of your personal data must be given voluntarily, specifically, consciously, and unambiguously. When it comes to giving one's consent to the provision of various services and the use of various tools through social media (such as cookies), it must be admitted that such consent forms are often not compliant with the requirements which have been set out for giving consent. For example, the user will often still not fully understand how their data will be used and to whom their personal information will be sent after they provide their consent by, most likely, clicking an 'OK' button.

2. The rights: your data, your choice

Your data counts. Your personal information is a form of currency, and for that reason it is valuable. Following any transaction with an authority, your information is processed, which involves sharing your personal details such as your name, address, or date of birth. Such information is also shared in the online environment every time you visit a website, use a search engine, sell or buy, use social media, send an email, or simply scroll, swipe, 'like', or post.

Data exchange makes life easier, more convenient, and smoother. However, you are the owner of your data. **Such data belongs to you**, which is why it is important for your data to be used in a manner in which you would reasonably imagine data processing to take place, and for such data to be retained and processed securely.

Your rights include the following areas:

The right to be **notified** of any processing of your personal data

- An authority must notify you when use is made of your personal data. You also have the right to know who is processing your personal data, along with how this is being done, from which sources such data will be take, the specific data involved, for which purposes such date is to be used, and on which legal bases it is to be used. For this purpose, any authorities must make available their privacy policies, and you are also entitled to send **enquiries** to any data processor in regard to your data.

- Several databases (such as the eesti.ee state portal or digilugu.ee) also enable you to check directly upon who has accessed your data.

The right to **refuse** data processing

- You often have the right to refuse data processing and the use of your data. Authorities and other organisations generally need your consent or another basis for processing your data. The state usually processes data based on legal requirements, in which case the consent of individuals is not necessary. Within the private sector it may also be claimed that video surveillance is in the legitimate interests of a business for example. If your consent is required for data processing, you may refuse at any time to grant such consent for processing.

- This also applies to the public sharing of any photos or videos of you. For example, before posting a photo or a video of another individual yourself, it is always polite to ask their permission first. You should also keep in mind the fact that such permission may be withdrawn at any time and you as the poster will then be required to remove the photo or video from social media.

- The bases for data protection include the following: the consent of the individual, a contract, a legal obligation, public duty, protection of the vital interests of an individual, or legitimate interest.

- **Spam**. Prior consent of the customer which can be withdrawn (such as through an unsubscribe link at the end of an e-mail) is also required for electronic direct marketing (which is regarded as a form of 'spamming'). Therefore, if you receive an email which has been sent to you for the purposes of selling you something, you may ask the company to stop sending you such emails or you can contact the Data Protection Inspectorate to have them look into the matter.

The right to **access** your data and to receive a **copy** of your data

- Your have the right to be notified when an organisation is using or retaining your personal data, while also having the right to access a copy of any data which may be collected.
- You have the right to request access to any data which may be collected by a company or a public authority. You also have the right to express your suspicions of any use of your personal data without due basis.

The right to **rectify** inaccuracies in your data

- You have the right to correct any incorrect or outdated information which concerns you which is in the possession of an organisation.

The right to be **forgotten**

- You have the right to ask an organisation to delete any data about you which is being retained or used without due basis. Please contact the initial source for the correction or removal of personal data. If you wish to restrict your data from being displayed by a search engine, you can fill in a specific form with Google, for example, to request the deletion of your personal data.
- Your identity belongs to you and you have the right to make any decisions concerning your image in the physical world, as well as in the digital world.

The right to the **transfer** of data

- You have the right to receive data which may have been collected about you by an authority, and in an accessible and readable format. This right allows you to request one company to transfer your personal data to another company whose services you wish to use in the future, but such a transfer must technically be possible and can only be done if the systems of the other company are compatible with those of the first one.

Automation-related rights

- If an automated decision has been made about you which has an unfavourable effect or legal consequences (such as, for example, such an automated decision which is handled by artificial intelligence) - that is, if a decision concerning you was not made by a human but is a profiling-based decision which was made by using information technology tools - then you have the right to request human intervention in the decision-making process, as well as the right to contest the decision and to rectify any of your personal data which may be incorrect or inaccurate.

The right to **object**

- If data regarding you is disclosed (such as via social media or general media sources) and such a disclosure damages your rights or freedoms, you have the right to submit your objections to the disclosing or posting party. In the event that this party refuses to respond to your objection within one month or they provide you with an unsatisfactory response, you may contact the Data Protection Inspectorate. You also have the right to turn for advice to the Human Rights Centre.
- In addition to turning to the disclosing party, you may also notify the social media platform via some form of notification procedure. If all of the above is unsuccessful, you may file a complaint with the courts against the disclosing party.
- Once you have submitted an objection or have disputed the processing of your personal data, you will have the right to request that any further processing of your personal data is henceforth restricted.
- If data regarding you may have been used to create a fake account, please report the identity theft to the police here: https://cyber.politsei.ee/.

For advice about data protection, please send us an email containing your questions or problems via the following address:

info@humanrights.ee

To **protect** your rights, you may submit an application directly to the data processor (such as the author of the post or the social media platform), file a complaint with the Data Protection Inspectorate, or turn to the courts. If you have any data protection or privacy-related problems or questions, please contact us for free consultation by sending an email to **info@humanrights.ee**.

3. Cyber-hygiene

Practice healthy online habits

The digitalisation of the world is accompanied by an increase in computer crime and cyber-operations. Any one of us can fall victim to cyber-crime, no matter what the aim of such operations, whether financial gain or political or social influencing. How can you prevent your computer from taking charge when you are using it?

Please review the following points in order to be able to protect yourself.

- **Privacy setting**
  Check the privacy settings and advertising-related settings for your accounts. Different applications and platforms may often be preconfigured so that your details are visible to all.

- Check whether you are comfortable with how your data may be being used and whether you would like to make any adjustments regarding which of your persona details is being shared with certain platforms and/or third parties.

- You should refrain from granting **access by default** when downloading certain applications. For example, does a game require your location data or access to your contacts. Probably not!

- **Secure** passwords and **two-factor** authentication

- Use secure passwords and update them regularly. You can use password managers (such as Keepass or Lastpass) in order to remember your passwords.

- Do not share your passwords with anyone.

- Two-factor authentication considerably improves the security of your accounts and is allowed by most applications and websites (including Facebook, Google, and many others).

- **Think before you share!**

- When you share information online, you should always keep in mind the fact that the information may be forwarded to strangers and could also be retained. Do not share anything about which you may later be embarrassed or which you would not want your parents or boss to see, for example. Before posting data, photos, or videos of other individuals, always ask their permission first. Delete their data if they no longer wish to have it disclosed on the internet. You should also avoid sharing email addresses with unauthorised persons and, if necessary, send blind copies instead.

- Make your accounts private and check your **friends list**.

- **Contribute to making the internet safer!** Set an example and report any hostility or harassment which you may have noticed online or the fact of anyone's data having been shared without their permission.

- Avoid **digital littering** and delete your old photos, documents, and emails occasionally.

- Always be **careful** when communicating with strangers and avoid sharing your personal contact details or photos with them. Not everything which shines online is gold, and an internet prince may sometimes turn out to be an internet villain.

- Never **lend money** over the internet and only use your credit card on reliable

websites. If your friend asks for a loan, use other channels (for example a phone call) to check whether the email which came from them really did come from them, and whether they are aware of what may have happened to their account.

- Be careful when opening **links or attachments**.
- Do not forget to regularly download **security updates** for your devices and applications.
- Prefer secure, password-protected WiFi **networks**.

Data leaks and privacy breaches: be aware of the more commonly-discovered online scams

When using the internet, you should keep in mind the probability that if something appears to be too good to be true, it probably is not true. Alluring scam schemes may be designed to earn money or to take over your user account or computer. Such schemes may be spread via email, social media sites, other websites, or chat rooms. **Please pay attention. Ensure you do not click without thinking, as each click has its consequences.**

Learn to recognise common scans and protect yourself from them.

Lotteries

Who would not want a free car or phone? Such lotteries may, however, be designed to earn clicks or money. Various forms of scheme can be used for this purpose.

1. In the case of one of the various schemes which are often used on different social media channels, you are notified that you have won the lottery, but are asked to pay a fee to take care of the paperwork or cover transmission costs if you attempt to claim your winnings.
2. If you submit your credit card information on a suspicious website, the information may end up in the hands of a fraudster who can use it to make online purchases.
3. In the case of some lotteries, you must share your telephone number and a code which is sent via text message which may, however, mean subscribing to a paid communications service, which itself results in an expensive phone bill instead of any winnings.
4. The 'like and win' fraud: this allows the owner of the website to easily directly advertising and scam schemes to you.

What should I do?

Who of us would not like to be able to make some easy money? The internet appears to provide numerous alluring opportunities to just this end. Unfortunately there are no free lunches. If something appears to be too good to be true, it usually is not true!

Make sure you never pay money for collecting your winnings online, and avoid sharing your credit card details on suspicious websites. If you would like to buy something online, prefer well-known companies and secure payment options such as, for example, use two different bank accounts (one of which is associated with your bank cards and another which can only be accessed via the online bank).

If you still want to take part in 'free' prize games, prefer those which have been organised by well-known companies. Pay attention to the content of the lottery (such as potential language errors, unclear terms and conditions, unrealistic prize amounts, or a website which is far too new) in order to be able to recognise fake lotteries.

A letter or message from a friend

If your friend's account has been hacked, you may receive a message which appears to be from your friend but is actually designed to extort money from you or to infect your account. This is done by manipulating your emotions in various ways such as, for example, by claiming that your friend is in trouble and urgently needs money. Such letters may also appear to come from strange 'princes' who are offering you an opportunity to make easy money.

What should I do?

If you receive a letter from a friend who claims to be in trouble, contact them via another means such as, for example, giving them a call. Ask whether the letter was actually from them and whether they are aware that their account is being used for sending such letters. If a friend sends you a link, ask them why they sent it before you attempt to open the link. When communicating online with strangers, you should always remain reasonable and careful.

Alluring connections

Fraudsters also use dating portals, and may spend quite a long time in building up a relationship. Suddenly, however, something catastrophic will happen to them (such as their life being in danger), and they will require a small loan from you. If the fraudster is in possession of some intimate photos or information, they may use it to blackmail you.

What should I do?

Be careful when communicating with strangers and do not share your private information without thinking about it, even if they appear to be very charming and open. Such fraudsters usually share the content and information which they have previously received from other victims. Never lend money to anyone whom you do not actually know.

Click magnets

Interesting fake offers or videos or images which attract your attention are often being used to direct any user who clicks on them to links which contain malware, resulting in their computer or smartphone being infected with malware which can harvest personal user information or financial information. This may make your computer slower and/or your account may start sending out strange posts which are additionally designed to infect the hardware of friends.

What should I do?

Choose carefully what you click on and, if something appears suspicious, you are very likely to find the information which you require via secure channels.

A warning from an IT Help Desk or bank employee

When it comes to receiving what appear to be official or expert warnings, an IT Help Desk may notify you of a theft, for example. You may be asked to change your passwords by clicking on what will turn out to be a fake link, even though it may look very similar to a certain online environment. When you click on the link, your computer may be infected with malware, while sharing your passwords may allow criminals to hijack your account. Such an approach may also mean that someone pretends to be a bank employee who asks you to provide the passwords which will make it possible for them to access your account.

What should I do?

Real websites never send you notifications from random accounts. It is also important to keep in mind the fact that a bank employee would never ask you over the phone to disclose your username, personal identification code, passwords, or credit card details (such as your card number and CVC code). Banks never remotely log into the online bank in the name of their clients. If you receive such a phone call, do not share your details with the caller. If you have already done so by accident, immediately notify the bank (by using a phone number which can be found on their website) in order to cancel your card and block any payments.

For advice about data protection, please send us an email containing your question or any problem which you may have:

info@humanrights.ee

INIMÕIGUSTE KESKUS

Luminate
Building stronger societies