Protection of privacy

Section 26 of the Constitution protects the right to the inviolability of private and family life, an inseparable part of which is the right to protection of personal data. In addition to the Constitution, processing of personal data is regulated by the European Union General Data Protection Regulation (GDPR), directly applicable as of May 2018. The principles laid down in the GDPR are further developed by the Estonian Personal Data Protection Act which entered into force on 15 January 2019.

The number of petitions received by the Chancellor concerning inviolability of private life increases year by year. In connection with establishment of the emergency situation, the Chancellor was also often asked about restrictions on processing of personal data. Relevant restrictions proportional in the narrow sense are inevitable in the fight against the coronavirus, but the right to inviolability of private life unquestionably still applies during an emergency situation (about the processing of personal data in an emergency situation, read the chapter on “Rule of law in an emergency situation”).

The media

Disclosure of data on private life in the media

The right to protection of private life is not absolute. The right to inviolability of private life may be restricted, for example, for protection of freedom of expression. Disclosure of personal data in the media is regulated by § 4 of the Personal Data Protection Act.

The media may disclose someone’s personal data if three main criteria are fulfilled simultaneously: public interest exists for disclosure of the data of the particular person, principles of journalism ethics are observed in disclosure, and disclosure of personal data does not cause excessive damage to the rights of the person. To disclose data, it is not merely sufficient to reach the conclusion that the public is in principle interested in a particular topic (e.g. spread of the coronavirus). Disclosure of personal data must contribute to debate on an important public issue, not merely to satisfy people’s curiosity or serve the business interests of a media publication.

Although the Chancellor is often contacted in connection with disclosure of personal data in

the media, supervision over private media publications is not within the Chancellor's competence. To such petitioners, the Chancellor can explain alternative ways for protection of their rights.

Processing of health data in an emergency situation is dealt with in the chapter on "Rule of law in an emergency situation". Disclosure of the data of children in the media is dealt with in the chapter on "Children and young people".

Recording devices

The number of petitions concerning recording devices and technical solutions enabling constant monitoring of people is growing year by year. People's concern for their privacy and for being alone free of monitoring must be taken seriously. No one likes an invasive environment of monitoring at their home, place of work or a rest area. A surveillance-free private life cannot become an inaccessible illusion. Any kind of monitoring must be justified and the people concerned must be aware of this.

The Chancellor has emphasised that privacy of residents must also be ensured in care homes. Video cameras in bedrooms in a care home may only be installed if video surveillance is necessary to ensure residents' own safety. For residents of a care home, the bedroom is their private area even when the room is shared with someone else. Processing of personal data (including subjecting someone to video surveillance) must be proportionate, fit for the purpose and minimal, as well as necessary for provision of a specific service. Video surveillance may be used if the desired aim cannot be achieved by other measures which are less invasive of a person's privacy. Consent of an individual themselves must exist for such an extensive surveillance activity as video surveillance in someone's bedroom (in more detail, see the chapter on "Inspection visits").

Use of cameras in the workplace must respect the principle that recording should interfere as little as possible with an employee's private life and human dignity. If no legitimate aim for recording exists, no recording may take place. Explanations have also been provided by the Data Protection Inspectorate on the use of video cameras in the workplace. The Inspectorate has also drawn up general guidelines on the use of cameras.

Recording in a police patrol vehicle

The Chancellor was contacted by a patrol officer asking to verify whether constant video and

audio recording in a patrol vehicle was compatible with the right to inviolability of private life under § 26 of the Constitution.

The Chancellor found that constant audio recording in a police patrol vehicle, without the possibility to switch it off, may indeed be excessive and violate the constitutional right to inviolability of private life. Recording in a patrol vehicle must have substantive justification and purpose. Fundamental rights may not be restricted more than can be justified by the aim sought.

The situation where conversation among police patrol officers during field work is constantly recorded seriously restricts the fundamental right of police officers to inviolability of private life. In line with the case-law of the European Court of Human Rights, private life cannot be interpreted narrowly. In work and occupational activity, the fundamental right to inviolability of private life is guaranteed to the extent that can be reasonably expected. Thus, police officers also have the right to inviolability of private life while in a service relationship.

A distinction should be drawn between video and audio recording. The distinction is justified since, by nature, simultaneous audio and video recording interferes more with private life than video recording alone. If sound is being recorded in a vehicle in addition to image, an individual must be notified of this. A sticker denoting video surveillance might not be sufficient to notify people who may find themselves in a patrol vehicle. It is suitable if a patrol officer orally notifies a person entering a patrol vehicle about audio recording, or if another means of notification (such as a sticker) is used in addition. The procedure for retention and use of recordings made in a patrol vehicle must be regulated and available to data subjects.

The Police and Border Guard Board (PBGB) promised that in 2020 an assessment would be carried out as to the need for recording in patrol vehicles used for different purposes. To ensure transparent data processing, the PBGB promised to improve regulations established by itself and, if necessary, make proposals to amend legislation. The PBGB promised to place stickers in patrol vehicles to notify police officers as well as third parties of the fact that both image and sound is being recorded in a police vehicle.

The state and data

Land register

The Law of Property Act establishes the principle of public access to the land register. No one

may excuse themselves by the fact of not being aware of the data in the land register. These principles have been unchanged since the re-establishment of the land register. However, over time the state has simplified the procedure of access to documents: land registry data that were initially available on paper are now kept electronically.

The Chancellor has earlier drawn the attention of the Ministry of Justice to the fact that the technical solution for queries in the land register may not excessively restrict people's right to inviolability of private life. The Ministry has analysed the issue of the land register and inviolability of private life, and has taken the results of the analysis into account in renewal of the land register. On that basis, no name-based queries can any longer be made in the publicly accessible information of the land register without self-authentication. According to the changes planned, the owner of an immovable will also be able to obtain information on who has accessed their data.

Commercial register and register of economic activities

The Commercial Code establishes the requirement to disclose data of sole proprietorships. The name and personal identification code of the sole proprietorship and the registered office of the enterprise must be entered in the commercial register. Entries in the commercial register are public. Everyone may examine the registry cards and business files, and obtain copies of registry cards and of documents in the business files. The requirement of disclosure of the data of a sole proprietorship has been established with a view to the credibility of general economic turnover and the interests of the undertaking's clients and partners.

Often, undertakings have no other choice than to register their business at their home address. If an undertaking does this, residence data become publicly available through the commercial register and they can be linked to a specific person. The Chancellor understands that this may annoy some sole proprietors.

The Chancellor has previously found that, based on the Constitution, it cannot be claimed that the requirement of disclosure of the address of an undertaking's registered office is, in itself, excessive and inadmissible. The requirement of disclosure must be proportionate to the aim sought.

The Chancellor requested an explanation from the Ministry of Economic Affairs and Communications as to whether disclosure of undertakings' data in several databases (commercial register, register of economic activities) in the present form is substantively

justified. If the aims for disclosure can be ensured in a manner less burdensome on undertakings, preference should be given to such a solution.

Massive transmission of data of people with disabilities

The Chancellor was asked to verify whether the Social Insurance Board was acting lawfully when sending to cities, towns and rural municipalities the personal data of people with disabilities living within their boundaries. The alleged aim of sending the data was to inform cities, towns and rural municipalities of people's possible need for assistance and help local authorities to plan and offer social services. In transmitting these data, the Social Insurance Board relied on § 13 of the Social Welfare Act under which it is required to notify a local authority of a person in need of assistance.

The Chancellor found that massive transmission of health data of people with disabilities under § 13 of the Social Welfare Act was not lawful. Technical requirements for processing personal data have also not been complied with in transmitting the data. It is understandable that the Social Insurance Board tries to help local authorities in supporting people with disabilities, but inviolability of private lives of individuals must also be respected. If a need arises to organise provision of social welfare services otherwise than what the Social Welfare Act enables, the law must be amended. People must be left the right to decline assistance and processing of their personal data.

Section 13 of the Social Welfare Act cannot be interpreted as allowing the Social Insurance Board to massively process the health data of people with disabilities for abstract purposes (e.g. to facilitate planning social services by rural municipalities, towns and cities). A disability merely in the context of services offered by a city, town or rural municipality does not necessarily mean a need for assistance. Individuals themselves are entitled to decide whether they wish to seek assistance and, in that connection, give the state the right to process data concerning their disability.

As far as is known, the Social Insurance Board has now stopped transmitting personal data. The Data Protection Inspectorate initiated supervision proceedings in relation to the incident.

Enabling access to data in the traffic register

Tartu City Government asked the Chancellor about access to traffic register data and asked her to verify whether the administrative practice of the Road Administration in releasing

these data complied with the practice of good administration.

Under the Traffic Act, local government bodies are entitled to obtain the necessary data from the traffic register to perform their statutory functions. To this effect, a local authority and the Road Administration enter into a contract. This is not a legislative act, so that the Chancellor is not competent to verify the conditions of the contract. If negotiations over the conditions of the administrative contract prove futile and the Road Administration blocks the city government's access to traffic register data, the city may have recourse to the court.

The Chancellor explained that under § 14 of the Constitution the right to good administration is one of the fundamental rights of individuals. A local authority is not a bearer of fundamental rights but their addressee, so that in its relations with the state a local authority may not rely on fundamental rights. However, good administration in the broader sense also includes categories of ethics and morals (politeness, readiness to help, etc.) which everyone must respect.

Business information portals

The Chancellor was also repeatedly asked about processing of personal data published in business information portals. Since these are undertakings in private law, the Chancellor is not competent to supervise their activities.

The Data Protection Inspectorate has initiated supervision proceedings to ascertain whether data processing by information portals complies with data protection rules and is compatible with the principles of personal data protection.

Disclosure of personal data and presumption of innocence

A petitioner contacted the Chancellor to assert that disclosure of personal data in the yearbook of the prosecutor's office violated the presumption of innocence and independence of judicial proceedings. Criticism was also directed against giving materials from a pending judicial case to a journalist.

Under § 22 of the Constitution, no one may be deemed guilty of a criminal offence before they have been convicted in a court and before the conviction has become final. Also, no one is required to prove their innocence in criminal proceedings. The requirement of presumption of innocence must be observed by police officers, prosecutors, judges and other public officials. The Supreme Court has emphasised that it is not compatible with the

presumption of innocence if a public authority draws public attention to the accused before a court judgment. The authority possessed by the state may give a different weight in the eyes of the public to information disseminated by a public authority. Therefore, one should be extremely careful with the choice of words and expressions in statements concerning charges.

Disclosure of personal data in the yearbook of the prosecutor's office is an activity in public law. The Chancellor explained that if inviolability of a person's private life has been violated or their honour or good name defamed, under § 9(1) of the State Liability Act they may claim financial compensation for non-pecuniary damage. The protection of honour and good name within the meaning of that provision also includes protection of the presumption of innocence. Also, in disputes over defamation of honour and good name, a distinction should be drawn between statements of fact and value judgments.

The Chancellor explained that journalists (like other private individuals) are indirectly bound by the requirement of presumption of innocence. Exercise of freedom of the press enshrined in § 45 of the Constitution entails duties and liability. Section 17 of the Constitution stipulates that no one's honour or good name may be defamed. Honour and good name can also be protected through civil procedure under the Law of Obligations Act. If someone finds that their honour and good name have been defamed in the media (e.g. through publication of an inappropriate value judgment or untrue statements of fact), they may have recourse to the court. If the court ascertains that a person's honour and good name has been defamed, it is possible to claim compensation for damage.

Under § 146 of the Constitution, the courts are independent in their activities and in discharging their duties and administer justice in accordance with the Constitution and the laws. As the main guarantee for judges' independence, § 147 of the Constitution stipulates that judges are appointed for life. Judges may be removed from office only by a court judgment. Constitutional guarantees enable judges to act independently when delivering a judgment and to administer justice without the fear of sanctions and pressure (e.g. by the media). The Supreme Court has emphasised that if courts have not agreed in their judgments with the version of events put forward by the defence, and the media has published materials about pending criminal proceedings, this does not automatically mean violation of presumption of innocence.

Disclosure of data of people having been in the service of occupation authorities

The Chancellor was contacted by an individual whose name was published in the *Riigi Teataja* gazette, as required by the Procedure for Registration and Disclosure of Persons who Have Served in or Co-operated with Security Organisations or Intelligence or Counterintelligence Organisations of Armed Forces of States which Have Occupied Estonia Act (the Occupation Act). Under the Act, information about service or cooperation must be disclosed in any case if the person did not submit a personal confession to the Internal Security Service within one year of the entry into effect of the Occupation Act (28 March 1995). The Occupation Act clearly and unequivocally lays down the possible consequences of failure to submit a confession. The Occupation Act does not lay down a procedure for erasure of personal data already disclosed.

The Chancellor explained that, prior to disclosure, the individual had the opportunity to examine documents held by the Estonian Internal Security Service proving their service in or cooperation with a security or intelligence organisation. Upon having examined the information, the individual could also have contested the information. The burden of proof of someone's service or cooperation rested on the Internal Security Service. The Chancellor cannot retroactively assess a person's past activity or its proof.

Information about the petitioner's service in the National Security Committee of the Estonian SSR has been public in the Appendix to the *Riigi Teataja* for 20 years. The Chancellor explained that if a person mentioned in the *Riigi Teataja* finds that continued disclosure of the information excessively restricts their right to the inviolability of private life, they should submit a relevant application to the Internal Security Service. If the Internal Security Service concludes that continued disclosure of personal data is justified and the individual's data is not removed from the *Riigi Teataja*, it is possible to file an action with the administrative court.