Office of the High Commissioner for Human Rights

Questionnaire on data protection

Contribution by Austria

Ad 1)

The right to safeguard one's privacy is covered in Austria's legal system by a number of statutory provisions governing specific aspects for its protection, inter alia:

- The fundamental right to respect the private and family life of article 8 of the European Convention on Human Rights (ECHR) and article 7 of the Charta of Fundamental Rights of the European Union (FRC) as well as the right to the protection of personal data in article 8 of the FRC. Both instruments are a yardstick for Austrian law;
- The (constitutional) law on the protection of the domiciliary right;
- Criminal law provisions: article 118 (violation of the privacy of correspondence and the suppression of correspondence) and article 118a (unlawful access to a computer system) in the Criminal Law Code; article 119 of the Code of Criminal Procedure (violation of the privacy of telecommunications), article 119a (abusive interception of data), article 120 of the Code of Criminal Procedure (abuse of audio recording or interception devices) and article 121 of the Code of Criminal Procedure (violation of occupational secrecy);
- Articles 77 and 78 of the Copyright Act (protection of correspondence and images);
- Article 77 and following of the Media Act (violation of the highly personal living spheres, protection against the disclosure of identity and protection against forbidden publication).

Under the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) of the Council of Europe, Parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data.

Within the European Union, the Data Protection Directive on the protection of individuals with regard to the processing of personal data (95/46/EC) ensures – among other legally binding instruments – that EU Member States protect individual fundamental rights and freedoms, in particular the right to privacy in the processing of personal data. This legal framework on the protection of personal data is currently under review by the EU.

At the national level, data protection is laid down explicitly as constitutional provision (sect. 1 (1) in the Austrian Data Protection Act 2000. The German text of this provision can be found under following link: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597).

In Austria personal data are widely defined as information relating to an identified or identifiable subject. This definition includes protection for all data which are communicated digitally. Specific provisions can apply to certain sectors, like e.g. for scientific research or statistics.

The Data Protection Act 2000 also contains detailed provisions on lawful processing of personal data. Data controllers and processors must for example comply with an appropriate technical and organizational standard to protect personal data against accidental or intentional destruction or loss, unauthorized disclosure or access and against all other unlawful forms of processing.

Ad 2)

The Austrian data protection authority (DPA, in German "Datenschutzbehörde") is an independent public authority charged with data protection as the Austrian supervisory authority for data protection. It is the equivalent to a national data protection commissioner in other countries.

In principle anybody can raise a complaint with the DPA. The DPA is authorized to investigate data applications in case of reasonable suspicion that a violation may have occurred. It has the power to request clarification from the data controller and inspect documentation. A violation of the right of an individual that his data will be kept secret, for rectification or deletion of data must be brought before the competent civil court. Failures to comply with the Act can be fined up to EUR 25,000.

Since the beginning of 2010, the Data Protection Act requires that a data controller notifies when data from his application have been unlawfully used in a systematic or material manner. Data controllers are only exempted from this obligation if the potential damage for the person, whose data were processed, is negligible or if costs incurred for such notification would not be reasonable.

Furthermore, in view of the constitutional character conferred to the provisions of the ECHR and the FRC, the rights laid down in these instruments are directly applicable constitutional law provisions before Courts and administrative authorities. They may be enforced before these bodies and, under certain conditions, also before the Constitutional Court. All laws must comply with constitutional laws; otherwise they may be repealed by the Constitutional Court. The legislator is therefore bound to these provisions.

Ad 3)

Regarding communication surveillance, interception and collection of personal data in the course of security police activities, the Security Police Act (SPA) specifically defines the prerequisites under which the security authorities are allowed to compile and process contact data.

In Austria are considered security police activities under the SPA the maintenance of public peace, order and security (*Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit)* (except for the local security police) and the duty to provide first general assistance (*erste allgemeine Hilfeleistungspflicht*). These tasks include in particular the aversion of danger, the preventive protection of legal interests and the search for wanted and missing persons and objects (§§ 16 and 19 et seqq. SPA).

Security authorities must already within the exercise of their general functions (§ 29 SPA) take into account the proportionality principle. This means that for investigation and surveillance purposes only the least severe means may be employed to achieve a legal aim. The Security Police Act also contains specific provisions with regard to the use of personal data within the framework of security police activities (§§51 seq

SPA). Security authorities are explicitly required to take into account also in this context the proportionality principle and must take adequate measures to safeguard the secrecy interests of persons concerned when using sensitive data or data relevant under criminal law. In addition, the security police has to comply with the provisions of the Data Protection Act 2000 (DPA) unless the SPA contains specific regulations in that respect.

Personal data may only be used by security authorities insofar as this is necessary to fulfil the tasks conferred upon them (§52 SPA). The subsequent paragraphs set out in detail for what purposes which personal data may be used in which manner. The relevant provision with regard to the surveillance of communications reads as follows:

"Admissibility of Processing"

§ 53. (1) - (3) […]

(3a) Security authorities shall have the right to request information from providers of public telecommunication services (§ 92 para. 3 (1) of the Telecommunications Act 2003-TKG 2003, Fed. Law Gazette vol. I no. 70) and other service providers (§3 (2) E-Commerce-Act –ECG, Fed. Law Gazette vol. I no. 152/2001)

1. on the name, address and subscriber number of a certain connection, if this is necessary for fulfilling the tasks conferred on them under this federal act,

2. on the Internet protocol address (IP-address) for a certain message and the time of its transmission, if they need these data as an essential prerequisite to avert

a) a concrete danger for the life, health or freedom of an individual within the framework of the duty to provide first general assistance (§19),

b) a dangerous attack (§ 16 para. 1 (1)), or

c) a criminal association (§ 16 para. 1 (2)),

3. on the name and address of a user to whom an IP address has been allocated at a certain time, if they need these data as an essential prerequisite to avert

a) a concrete danger for the life, health or freedom of an individual within the framework of the duty to provide first general assistance (§19),

b) a dangerous attack (§ 16 para. 1 (1)), or

c) a criminal association (§ 16 para. 1 (2)), even if the use of stored data is required for that purpose pursuant to § 99 para. 5 (4) in conjunction with § 102a TKG 2003,

4. on the name, address and subscriber number of a certain connection by reference to a conversation held on this line by naming as exactly as possible the point of time and the passive subscriber number, if this is necessary for fulfilling the duty of providing first general assistance or fore averting dangerous attacks.

(3b) if it is to be assumed on the basis of specific facts that there is a current danger for the life, health or freedom of an individual, the security authorities are entitled, for the purpose of providing assistance or averting the danger, to require operators of public telecommunication services to provide information about location data and the International Mobile Subscriber Identity (IMSI) of the terminal equipment carried by the endangered person or anyone accompanying that person, even if the use of stored data is required for that purpose pursuant to § 99 para. 5 (3) in conjunction with § 102a TKG 2003, and to apply technical means for localizing the terminal equipment.

(3c) In the cases of paras. 3a and 3b, the security authorities are responsible for the legal admissibility of the request for information. The requested body shall be obliged to provide the information without delay and, in the case of para. 3b, against payment of pursuant to the Regulation on Surveillance Costs (*Überwachungskostenverordnung-ÜKVO*, Fed. Law Gazette vo. II no. 322/2004 In the case of para. 3b, the security authorities must in addition forward to the operator without delay, not later than within 24 hours, a written documentation. In the cases of para. 3a (3) and para. 3b, the security authority shall be obliged to inform the person concerned that information has been obtained for the assignment of his/her name or address to a certain IP address (§ 53 para. 3a (3) or for his/her localisation (§ 53 para. 3b), if the use of stored data is required for that purpose pursuant to § 99 para.

5 (3) or (4) in conjunction with § 102a TKG 2003. They shall inform the person concerned as soon as possible in a provable manner of the legal basis as well as the date and time of the request. The information of the persons concerned can be postponed as long as the purpose of the compilation would be endangered by it, and it need not be given, if it can be proved that the person concerned has already been informed or it is impossible to inform the person concerned.

(3d) - (5) […]

The surveillance of the content of a communication is not possible under the SPA. Moreover, the proportionality principle must in any event be taken into account by the security authorities. Hence, arbitrary interferences with the privacy, family, home or correspondence of a person are impeded.

The confiscation of letters, information about data of a message transmission, as well as surveillance of messages is legally solely possible under the circumstances provided in §§ 134 et seq. CPC (Code of Criminal Procedure), e.g. in case of kidnapping, hostage-taking, prevention/clearance of a crime. In general, it shall be ordered by the public prosecutor on the basis of a court authorization. Investigative measures may be ordered only for the period that is likely to be required in order to fulfil the purpose. Subsequent orders can be taken, whenever it is to be expected on account of certain facts that the further performance of an investigative measure will lead to success. Investigative measures shall be cancelled if the conditions which led to their enactment are no longer met. Surveillance measures shall only be admissible to the extent that proportionality is maintained.

Furthermore, the accused shall be given an opportunity to see and hear all results. The persons concerned by the performance of investigative measures shall have the right to examine the results whenever they relate to their data of a message transmission, to messages addressed to them or sent by them, or to conversations conducted by them, or to images showing them. The public prosecutor shall inform these persons of this right and their right under paragraph (4), to the extent that their identity is known, or can be established without particular effort. (The relevant provisions of the CPC are enclosed in *Annex 2*)

Referring to personal data and subscriber information, § 76a CPC states, that the Service Provider has to provide subscriber information of a static IP address to the police or judicial authority in case of a criminal investigation, if there is a concrete suspicion of a crime (regardless of its severity). A request from a police authority will be sufficient. Subscriber information of a dynamic IP address has to be provided only upon a written order of the public prosecution service in charge, which has to state the reasons, as well. In urgent cases, oral orders followed by a written order will be accepted.

However, law enforcement authorities may not obtain any traffic data that has been retained for more than six months prior to the request and may not obtain subscriber information if the IP address may refer to more than 10 people. Definitions regarding subscriber information, IP address, traffic data etc. are stated in the Austrian „Telecommunication Act 2003“.

Ad 4)

The right to file a complaint with the independent Data Protection Authority under § 90 SPA and § 26 DPA provides an effective and adequate protection against interferences in the meaning of Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. Furthermore the SPA established an independent, effective domestic oversight mechanism ensuring the transparency communication surveillance by the State.

The SPA contains specific provisions for legal protection of individuals against measures by the security police in Part 6.

Data Protection Authority

Under § 90 SPA any person concerned may file a complaint with the independent Data Protection Authority because of a violation of rights as a result of the use of personal data in matters of security administration.

Moreover, under the legal protection provisions of the Data Protection Act 2000, any person may, even in case of a mere suspicion of an (unnoticed) data compilation by a security authority, file a request with the competent security authority/authorities for a pertinent information concerning him/her. If the information received is not considered to be fully satisfactory, the person can file a complaint before the independent Data Protection Authority in accordance with § 26 of the DPA 2000.

Legal Protection Commissioner

An independent Legal Protection Commissioner has been established at the level of the Federal Ministry of the Interior. He is also responsible to provide legal protection for persons (§§ 91a to 91d SPA). Only persons, who have special qualifications and experience in the field of fundamental and freedom rights and have practised for at least five years a profession for the exercise of which completion of law studies is required, can fulfil this task. In his former and current professional activities he must display a close affinity with fundamental and freedom rights.

The SPA enumerates exhaustively the protection measures the Legal Protection Commissioner can provide for the compilation of personal data protection (§ 91c SPA). The security authorities are obliged to notify the Legal Protection Commissioner any surveillance of communications measures taken by them and setting out the relevant reasons for them. The Legal Protection Commissioner must subsequently subject these measures to a control by reviewing their compliance with the law. In case that the use of personal data would violate the rights of persons concerned, the Legal Protection Commissioner is obliged either to inform the persons concerned, if they have no knowledge of this use of data, or file a complaint with the Data Protection Authority, if no information can be provided because of certain reasons as for instance the rights of third persons or the protection of overriding security interest. The exemption are specifically listed in § 26 para. 2 of the Data Protection Act 2000.

Under § 91d para. 1 SPA, security authorities shall also give the Legal Protection Commissioner an opportunity to inspect at any time all the necessary documents and records, and (having regard to national security and safety of persons) must make available all the information needed. Moreover, under § 91d para. 2 SPA they shall also give the Legal Protection Commissioner an opportunity to supervise at any time the implementation of the measures mentioned in § 91c, and to enter all rooms where recordings or other surveillance results are stored.

Austrian Ombudsman

Moreover, § 147 CPC authorizes the Austrian Ombudsman to review and investigate those orders by the public prosecutors, the judicial approvals and their implementation, if certain requirements are met.

Constitutional Court

In general, individuals who consider that their constitutionally guaranteed right to data protection has been infringed by a decree or through the application of illegal norms can apply to the Austrian Constitutional Court.

Ad 5)

Austria, Liechtenstein, Slovenia and Switzerland have submitted a joint-statement to this question. The statement is enclosed in *Annex I*.

ANNEX 1

Common response of Austria, Liechtenstein, Slovenia and Switzerland to the OHCHR request regarding „The right to privacy in the digital age“ (dated 26 February 2014)

Issue 5: “Any other information on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data”

The mandate given by General Assembly resolution 68/167 to the UN High Commissioner for Human Rights to submit a report on the right to privacy in the digital age provides an important and timely opportunity to submit legal and policy considerations that will help the international community to make much-needed progress. **In this context, Austria, Liechtenstein, Slovenia and Switzerland would like to jointly highlight the following aspects**:

During the last years, international media outlets have reported extensively about far-reaching practices involving domestic and extraterritorial surveillance, interception of digital communications and the collection of personal data, including on a mass scale and without any showing of need or probable cause. These revelations have raised serious concerns among governments, civil society, the private sector and the public at large regarding the legal and policy implications of these practices. The concerns expressed relate primarily to the right to privacy, though other fundamental rights (such as the right to freedom of expression and the right to non-discrimination) are also at stake, as are other norms of international law. Austria, Liechtenstein, Slovenia and Switzerland therefore fully support UN General Assembly Resolution 68/167, which calls upon States to “respect and protect the right to privacy, including in the context of digital communication” and suggest a number of concrete measures for this purpose.

Respecting and protecting the right to privacy in the digital age is a formidable long-term challenge. In this context, the upcoming report by the UN High Commissioner for Human Rights can provide crucial views and recommendations. Such guidance is particularly necessary as there is currently very limited material to draw from at the inter-governmental level, and jurisprudence on the core issues at hand is either not existent or not publicly available, not least due to the secret nature of relevant activities. Going forward, an open discussion on the concrete legal and policy parameters of the right to privacy in the digital age will be necessary and has indeed started, as evidenced by the expert seminar held in Geneva on 24-25 February 2014.

(1) Understanding the right to privacy

GA Resolution 68/167 refers to the right to privacy as the right “according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights”. The right to privacy clearly applies to activities both in the physical environment as well as in the digital sphere. Interferences with the right to privacy or the sanctity of correspondence are only lawful to the extent that they are provided by law, justified in the public interest or for the protection of the fundamental rights of others and

proportionate. It is immaterial for this proportionality test whether or not a person subject to surveillance, interception or data collection may be aware of the existence of such measures. Some States, however, tend to apply a very narrow interpretation of the scope of the right to privacy, and/or an overly broad interpretation of legitimate limitations. The High Commissioner's report should therefore pay great attention to these important aspects and should focus on what forms of interference are "arbitrary".

(2) Extraterritorial surveillance, interception and data collection

GA Resolution 68/167 specifically refers to the extraterritorial dimension of interferences with the right to privacy. The nature of modern communication technology is such that even seemingly local communications – their content as well as related metadata – can be accessed from elsewhere in the world. In today's digital age, the right to privacy is, broadly speaking, under greater threat from abroad than from within a State. This is *inter alia* due to the fact that States typically apply more stringent restrictions to domestic surveillance, interception and data collection, and that States generally simply collect more data abroad, especially in a national security context. This raises the crucial question of whether and to what extent States are obliged by article 17 ICCPR to respect and protect the right to privacy in the context of extraterritorial surveillance, interception and data collection. During the negotiations leading to the adoption of GA Resolution 68/167, States informally advanced different views in this regard. Austria, Liechtenstein, Slovenia and Switzerland therefore hope that the High Commissioner's report will provide guidance on this crucial question. Such guidance should take into account the following:

- The Human Rights Committee has already recognized that there are situations in which the obligations under the ICCPR apply extraterritorially. General Comment No. 31 on the nature of the general legal obligation imposed on States Parties to the Covenant stated that States Parties "must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party. […] This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained."
- This principle also applies, *mutatis mutandis*, to the actions of a State Party whereby it interferes extraterritorially with the right to privacy of a person. In such situations, the protected value associated with that person, namely his or her privacy, is indeed under the effective control of that State. While the General Comment No. 31 was clearly formulated against the background of past cases involving various degrees of physical control by a State Party over a person outside its territory, the underlying logic of the principle stated therein makes it applicable to situations of <u>partial</u> control, i.e. control over certain aspects of a person's human rights.
- In other words, the extraterritoriality of States Parties' human rights obligations is not categorical. A State Party is subject to some human rights obligations even in situations in which it does not exercise full physical control over an individual and the entire corpus of human rights. If it exercises effective control over the ability of the individual to enjoy that right, then the obligation applies extraterritorially.

(3) The role of the Human Rights Committee

As outlined above, the right to privacy in the digital era raises important issues regarding the interpretation of the ICCPR. Austria, Liechtenstein, Slovenia and Switzerland would therefore support any efforts by the Human Rights Committee to pronounce itself on related matters, in particular by updating its relevant General Comments (GC), primarily GC no. 16, further also GC no. 31. Most importantly, the Human Rights Committee should work to translate the concepts and principles of effective control in the physical world into a standard of virtual control over the right to privacy and its related rights in the digital world.

(4) The role of Special Procedure mandate holders

Austria, Liechtenstein, Slovenia and Switzerland are convinced that those Special Rapporteurs whose mandates are concerned with the right to privacy and the issue of national security practices (such as the UN Special Rapporteurs on the right to freedom of opinion and expression, and on human rights and fundamental freedoms while countering terrorism) should be encouraged to come together for a joint initiative and issue for example guidelines clarifying the legal regimes, and develop best practices on ensuring respect for the right to privacy in the digital age. In full support of Human Rights Council (HRC) Decision A/HRC/25/L.12 convening a panel discussion on the promotion and protection of the rights to privacy in the digital age in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale at the 27th Session of the HRC, the contributions of Special Rapporteurs will be very important to inform and further this important debate.

9 April 2014

ANNEX 2

§ 134 CPC (Definitions)

For the purposes of the present law, the following terms shall mean:

1. "confiscation of letters" relates to telegrams, letters or other mail pieces that are opened or held back, which the accused sends off, or which are addressed to him/her,

2. "information about the data of a message transmission" is information that is provided about communication data (§ 92 (3) item 4 of the Telecommunications Act), access data (§ 92 (3) item 4a of the Telecommunications Act) and position data (§ 92 (3) item 6 of the Telecommunications Act) of a telecommunications service, or a service of the information society (§ 1 (1) item 2 of the Notification Act),

3. "surveillance of messages" is the determination of the contents of messages (§ 92 (3) item 7 of the Telecommunications Act), which are exchanged or forwarded via a communications network(§ 3 item 11 of the Telecommunications Act), or a service of the information society (§ 1 (1) item 2 of the Notification Act),

4. "optical and acoustic surveillance of persons" is the surveillance of the conduct of persons by penetrating their private sphere, as well as of the comments of persons which are not intended to come to the immediate knowledge of third parties, by using technical means for image and sound transmission and image and sound recording, without the persons concerned having any knowledge thereof,

5. "result" (of the confiscation, information or surveillance listed in items 1 to 4) is the contents of letters (item 1), the data of a message transmission, or the contents of transmitted messages (items 2 and 3), and the image and sound recordings of a surveillance operation (item 4).

§ 135 CPC (Confiscation of Letters, Information about Data of a Message Transmission, as well as Surveillance of Messages)

(1) The confiscation of letters shall be admissible if it is required to clear up a punishable act, committed with intent, which carries a prison term of more than 1 year, and if the accused is being kept detained for such an act, or if his presentation in court or arrest has been ordered for this purpose.

(2) Information about the data of a message transmission shall be admissible

1. if and as long as it is urgently suspected that one of the persons concerned by the information has kidnapped or otherwise seized another person, and that the information about

data is restricted to such a message of which it has to be assumed that it was communicated, received or sent by the accused at the time when the person was deprived of his/her liberty,

2. if it is to be expected that this can promote the clearing up of a punishable act, committed with intent, which carries a prison term of more than six months, and if the owner of the technical equipment, which was or will be the source or the target of a message transmission, expressly agrees to it, or

3. if it is to be expected that this can promote the clearing up of a punishable act, committed with intent, which carries a prison term of more than one year, and if it is to be assumed, on account of certain facts, that data concerning the accused can thus be obtained.

(3) The surveillance of messages shall be admissible

1. in the cases of paragraph (2) item 1,

2. in the cases of paragraph (2) item 2, whenever the owner of the technical equipment, which was or will be the source or target of the message transmission agrees to the surveillance,

3. if this appears to be required to clear up a punishable act, committed with intent, that carries a prison term of more than one year, or if the clearing up or prevention of a punishable act, committed or planned within the framework of a criminal or terrorist association or a criminal organisation (§ 278 to § 278b of the Criminal Law Code) would otherwise be essentially impeded, and

a. the owner of the technical equipment, which was or will be the source or target of messages is urgently suspected of a punishable act, committed with intent, that carries a prison term of more than one year, or of a punishable act pursuant to § 278 to § 278b of the Criminal Law Code, or

b. it is to be expected, on account of certain facts, that a person urgently suspected of the offence (letter a) will use the technical equipment or will establish contact with it;

4. if it is to be expected, on account of certain facts, that the whereabouts of a fugitive or absent accused may be determined, who is urgently suspected of a punishable act, committed with intent, that carries a prison term of more than one year.

§ 136 CPC (Optical and Acoustic Surveillance of Persons)

(1) The optical and acoustic surveillance of persons shall be admissible

1. if and for as long as it is urgently suspected that a person affected by the surveillance has kidnapped or otherwise seized another person, and if the surveillance is restricted to processes and comments at the time and location of the deprivation of liberty,

2. if it is restricted to processes and comments that are intended to be brought to the knowledge of an under-cover investigator, or another person informed of the surveillance, or that may be perceived by that person directly, and if it appears to be required in order to clear up a crime (§ 17 (1) of the Criminal Law Code), or

3. if the clearing up of a crime carrying a prison term of more than ten years, or of a crime by a criminal organization or terrorist association (§ 278a and § 278b of the Criminal Law Code), or the clearing up or prevention of a punishable act committed or planned within the framework of such an organization or association, or the determination of the whereabouts of the person accused of such a punishable act would otherwise be without prospects of success or be essentially impeded, and

a. the person who is the target of the surveillance is urgently suspected of a crime carrying a prison term of more than ten years, or of a crime pursuant to § 278 a or § 278b of the Criminal Law Code, or

b. it is to be expected, on account of certain facts, that a person who is thus urgently

suspected will establish contact with the person who is the target of the surveillance.

(2) To the extent that this is unavoidable for performing the surveillance pursuant to paragraph (1) item 3, it shall be admissible to penetrate a certain flat or other rooms protected by domestic authority, if it is to be expected, on account of certain facts, that the accused will use the rooms in question.

(3) The acoustic surveillance of persons in the process of clearing up a punishable act is also admissible

1. if it is restricted to processes outside of a flat or other rooms protected by domestic authority, and if it is conducted exclusively for the purpose of monitoring objects or premises in order to record the conduct of persons who enter into contact with the objects, or who enter the premises, or

2. if it is performed exclusively for the purpose mentioned in item 1 in a flat or other rooms protected by domestic authority, and the clearing up of a punishable act, committed with intent, that carries a prison term of more than one year, would otherwise be essentially impeded, and the proprietor of that flat or those rooms expressly agrees to the surveillance.

(4) A surveillance shall only be admissible to the extent that proportionality (§ 5) is maintained. A surveillance pursuant to paragraph (1) item 3 to prevent punishable acts, committed or planned within the framework of a terrorist association or a criminal organization (§ 278a and § 278b of the Criminal Law Code) shall only be admissible if one may conclude from certain facts that there is a serious danger to public security.

§ 137 CPC (Common Provisions)

(1) The criminal police may conduct a surveillance pursuant to § 136 (1) item 1 on its own initiative. The other investigative measures pursuant to § 135 and § 136 shall be ordered by the public prosecutor on the basis of a court authorization, with the entering of rooms pursuant to § 136 (2) always requiring a court authorization in each individual case.

(2) § 111 (4) and § 112 shall be applied in analogy to the confiscation of letters.

(3) Investigative measures pursuant to § 135 and § 136 may only be ordered for such a future period of time (in the cases of § 135 (2) also for such past periods of time) that are likely to be required in order to fulfil the purpose. Another order is admissible in every case, whenever it is to be expected on account of certain facts that the further performance of an investigative measure will lead to success. Moreover, the investigative measure shall be ended as soon as its requirements have ceased to apply.

§ 138 CPC

(1) Orders and court authorizations for the confiscation of letters pursuant to § 135 (1) shall indicate the designation of the proceedings, the name of the accused, the offence of which the accused is suspected and its statutory designation, as well as the facts from which it results that the order or the authorization is required and proportional in order to clear up the offence. An order and authorization of an investigative measure pursuant to § 135 (2) and (3), as well as § 136 shall also contain the following:

1. the name or other identification features of the proprietor of the technical device that was or will be the origin or target of a message communication, or of the person whose surveillance is being ordered,

2. the premises envisaged to carry out the investigative measure,

3. the type of message communication, the technical equipment and the terminal device, or the type of the technical means that is likely to be used for the optical and acoustic surveillance,

4. the time when the surveillance begins and ends,

5. the premises which may be entered on the basis of the order,

6. in the case of § 136 (4) the facts from which results the serious danger to public security.

(2) Operators of postal and telegraph services are obliged to cooperate in the confiscation of letters and, upon an order by the public prosecutor, hold back such mailings until a court authorization has been received; if such an authorization is not granted within three days, they must not postpone the delivery any further. Providers (§ 92 (1) item 3 of the Telecommunications Act) and other providers of services (§ 13, § 16 and § 18 (2) of the Ecommerce Act, Federal Law Gazette I No. 152/2001) are obliged to provide information about data of a message transmission (§ 135 (2)) and to cooperate in the surveillance of messages (§ 135 (3)).

(3) The obligation pursuant to paragraph (2) and its scope, as well as a possible obligation to keep confidential facts and processes linked to the order and the authorization shall be imposed upon the provider by the public prosecutor by means of a separate order. This order shall indicate the corresponding court authorization. § 93 (2), § 111 (3), as well as the provisions on searches shall apply in analogy.

(4) The public prosecutor shall review the results (§ 134 item 5) and have those parts transformed into images or written form, as well as annexed to the files that are of significance for the proceedings and may be used as evidence (§ 140 (1), § 144, § 157 (2)).

(5) After ending an investigative measure pursuant to § 135 (2) and (3), as well as § 136, the public prosecutor shall immediately serve his/her order and the court authorization on the accused and the persons concerned by the investigative measure. However, the service may be postponed for as long as this would jeopardize the purpose of these or other proceedings. If the investigative measure was begun later or ended earlier than at the times indicated in paragraph (1) item 4, the period of the actual performance shall also be communicated.

§ 139 CPC

(1) The accused shall be given an opportunity to see and hear all results (§ 134 item 5). Whenever the interests of third parties so require, the public prosecutor shall, however, exclude from becoming known to the accused those parts of the results that are not of significance for the proceedings. The foregoing shall not apply whenever the results are being used during the trial.

(2) The persons concerned by the performance of investigative measures shall have the right to examine the results whenever they relate to their data of a message transmission, to messages addressed to them or sent by them, or to conversations conducted by them, or to images showing

them. The public prosecutor shall inform these persons of this right and their right under paragraph (4), to the extent that their identity is known, or can be established without particular effort.

(3) Upon application by the accused, further results in image or written form shall be transformed if this is of significance for the proceedings and their use as evidence is admissible (§ 140 (1), § 144, § 157 (2)).

(4) Upon application by the accused or ex officio the results of the investigative measure shall be destroyed if they cannot be of significance for criminal proceedings, or may not be used as evidence. The persons concerned by the investigative measure also have this right of application, to the extent that these are messages or images showing them, which are addressed to them, or sent by them, or conversations conducted by them.

§ 140 CPC

(1) Results (§ 134 item 5) may only be used as evidence, and will otherwise be null and void,

1. if the requirements for an investigative measure pursuant to § 136 (1) item 1 prevailed,

2. if the investigative measure pursuant to § 135 or § 136 (1) items 2 or item 3 or paragraph (3) was lawfully ordered and authorized (§ 137), and

3. in the cases pursuant to § 136 (1) items 2 and 3 only to prove a crime (§ 17 (1) of the Criminal Law Code),

4. in the cases of § 135 (1), (2) items 2 and 3, (3) items 2 to 4 only when used as evidence for the punishable act, committed with intent, for which the investigative measure was ordered or could have been ordered.

(2) If a review of the results leads to indications that another punishable act was committed than the one that gave rise to the surveillance, a separate file must be opened with that part of the results, whenever their use as evidence is admissible (paragraph (1), § 144, § 157 (2)).

(3) Results may only be used in other judicial proceedings or in proceedings before administrative authorities to the extent that their use was or would be admissible in criminal proceedings.

§ 141 CPC (Data Matching)

(1) For the purposes of the present law, "data matching" means to compare, by using electronic support (§ 4 item 1 of the 2000 Data Protection Act), data from one data application, which contain specific features characterizing or excluding an alleged offender, to data from another data application, which contains such information, in order to determine persons who fall within the group of suspects, on account of these features.

(2) Data matching shall be admissible if the clearing up of an offence (§ 17 (1) of the Criminal Law Code) would otherwise be essentially impeded, and if only such data are included that courts, public prosecutors and security authorities have already investigated or processed for the purposes of already pending criminal proceedings, or otherwise on the basis of existing federal or regional laws.

(3) Whenever the clearing up of a crime carrying a prison term of more than ten years, or a crime pursuant to § 278a or § 278b of the Criminal Law Code would otherwise be without prospects of success, or be essentially impeded, it is admissible to include data into such data matching operations that have to be forwarded to the courts and public prosecutors, and to the criminal police pursuant to § 76 (2), as well as data about persons who have obtained goods or services from a certain company, or who are members of private-law associations of persons, or of legal, private-law or public-law entities.

(4) Sensitive data (§ 4 item 2 of the 2000 Data Protection Act) must not be included in a datamatching operation. The foregoing shall not apply to data concerning nationality, nor to data to designate a group of perpetrators according to the features of an offence, or data that public prosecutors or security authorities have lawfully established by means of record department measures, by searching a person, by physical examination or by moleculargenetic analysis, whenever these data are used exclusively for datamatching operations pursuant to paragraph (1). The data concerning associations of persons, the purpose of which is directly connected to one of the especially protected features must never be used for data matching.

§ 142 CPC (Data-Matching Operations)

(1) The public prosecutor shall order a data-matching operation on the basis of a court authorization. The public prosecutor or the criminal police shall transcribe the result of the data-matching operation into written form, to the extent that it is of significance for the proceedings.

(2) In addition to the information indicated in § 102 (2), the order for a data-matching operation, as well as its court authorization shall contain the following data:

1. the designation of those features, for which a match is sought,

2. the data application (§ 4 item 7 of the 2000 Data Protection Act) and those of its data that comprise the sought features,

3. the ordering party required to forward the data (§ 4 item 4 of the 2000 Data Protection Act).

(3) An order pursuant to paragraph (2), together with its court authorization, shall be sent to the Data Protection Commission and all persons who have been found by way of the datamatching operation. However, service on the identified persons may be postponed for as long as it might jeopardize the purpose of the current or other pending criminal proceedings.

(4) The Data Protection Commission shall have the right to file a complaint pursuant to § 87 against the court authorization of an order pursuant to paragraph (2).