General Data Protection Regulation – Code of Conduct for Internet Service Providers

Version 1.1. v. 16.06.2020

ISPA – Internet Service Providers Austria

Währinger Straße 3/18
1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
🌐 www.ispa.at
Preamble

The General Data Protection Regulation (GDPR) is in force in Austria since May 25, 2018 and is directly applicable. Its target is to protect natural persons with the processing of their personal data and to unify data protection standards in Europe.

The undersigned companies do acknowledge their responsibility with regard to the fundamental right to data protection and expressly admit to their social responsibility within the scope of their business.

The elaboration of a common basic understanding of the requirements and obligations which the GDPR contains for ISPs and the sector-specific compliance as well as the performance of necessary specifications together with the transmission of this understanding to the customers shall guarantee the best possible implementation of the GDPR as well as legal certainty for the ISPs. These rules of conduct specify the application of the GDPR. Due to the fact that the stipulations of the Telecommunications Act for ISPs have to be considered regarding many data protection-relevant questions, these shall equally be covered with regard to the sector-specific specifications.

For this reason, the Internet Service Providers Association Austria (ISPA) as the representative of the Austrian Internet industry has elaborated the following rules of conduct according to Article 40 GDPR in cooperation with its members and other leading stakeholders, which if required and upon re-submission to the Data Protection Authority may be further developed and supplemented.

Scope of application

Internet service providers who provide public communication networks or -services and who dispose of a common authorization in terms of section 15 TKG (Austrian Telecommunications Act), may subject to these rules of conduct (see item VII below).
I. Infrastructure-related service relations

1. In context of the performance of communication services to end customers, the one operator who holds the contractual end customer relationship regularly is the controller, the end customer is the data subject. To enable end customers to use communication services beyond the limits of the infrastructure of their contracting partner, it is necessary for operators to ensure by contractual and technical arrangements that the end customer services may be seamlessly performed beyond network borders.

2. To guarantee such use, the cooperation of the operators is subjected to a sector-specific system of rules which on the European level provides a frame by various guidelines and regulations and which is implemented in national laws (such as the Telecommunications Act 2003 in Austria). In addition to the obligations which apply to all operators (such as the obligation to interconnection), there are specific access obligations for market dominating operators.

3. According to the sector-specific European legal frame, the operators are also subject to a narrow legal regime regarding the design of their business models. This particularly includes the regulation of competition, frequencies, universal service and consumer protection as well as sector-specific data protection provisions.

4. Based on a sector-specific system of rules voluntary and obligatory access- and connection services (“ISP-services”) have developed, which are being offered and demanded on the (wholesale-) market. In the end these rules ensure the functioning of the entire market, the exchange of information via the top of the network of a single operator and ensure that operators who do not have the necessary infrastructure, get access to external infrastructure and are thereby enabled to offer their products and services to their end customers.

5. In the context of performing ISP-services between operators, personal data of end customers are being processed. The processing of these data is necessary in order to allow the classical business model of an operator, which is designed as follows:

6. Contracting partners in the provision of ISP-services are always two operators, who do not necessarily, but potentially have their own end customer relationships. In this specific performance relationship, no contractual relations exist between the end customer of an operator and the other operator involved. Every operator providing an ISP-service (“operator”) processes personal data of the end customer of the demander of the ISP-services (“demander”) within his network in accordance with his own specific statutory obligations, data protection management systems and data security requirements. These data need to be processed to be able to provide the ISP-service.

7. In those cases where the ISP-services are exclusively based on the sector-specific legal framework, the means and purposes of the data process are determined solely by the respective regulation standards. The role of the controller in terms of Art. 4 subparagraph 7 GDPR is thus determined according to the criteria of the national regulation standards. Respective regulatory obligations exist particularly in sections 92 ff TKG (Austrian Telecommunications Act) as well as in the regulatory decisions of the Austrian Telecom Control Commission (TKK), which stipulate and even command in detail the processing of personal data of end users within the scope of ISP-services.

8. In terms of the relation of the operators vis-à-vis each other, no reciprocal decisional authority exists regarding data processing. At the same time the demander basically has no option to choose the operator but is bound to that one operator who offers the ISP-services necessary for the provision of end customer services, resp. who owns the necessary infrastructure. Thus, no processing relationship in terms of Art 28 GDPR is being established between the demander and the operator. No processing of data beyond the purpose of the ISP-service is done by the performer of the ISP-service in its own interest. Means and purposes of the data processing are rather exclusively defined by the national and European regulatory standards.

Controller of the data processing within the scope of the performance of end customer services shall therefore remain the operator who holds the end customer contractual relationship. The performer of the ISP-services on the other hand shall be solely responsible for compliance with statutory data protection- and data security provisions and shall explicitly not be subjected to any decisional authorities (such as data-security measures).
It shall equally be stated that no joint controllership according to Art 26 GDPR exists between the operators, as purposes and means are not jointly determined. As described above, personal data are processed by each operator subject to its own determined purposes with the means determined by each operator resp. by common standards.

9. In relation to the end customer the operator who holds the contractual end customer relation will regularly be the controller, the end customer will be the data subject. The same applies to the relation vis-à-vis business customers who themselves act as controllers with respect to their own data applications. When offering traditional communication services (internet access, telephony...) the operator shall not be subject to any decisional authority of the end user, but exclusively processes personal data on the basis of statutory and regulatory standards in order to be able to perform the service. Therefore, no processing relation in terms of Art 28 GDPR is being established.

No joint controllership according to Art 26 GDPR exists either in this case between the operator and the end customer. The operator solely determines all purposes and means of the data processing.

In exceptional cases the offer of special- or additional services may however create a processing relation. This shall however be examined individually on a case-by-case basis, whereby a possible contractual decisional authority regarding data processing shall be specifically considered.

10. In addition to those service relations where means and purposes of the data processing are exclusively determined by national and European regulation standards, further access- and connection services exist, which are carried out according to the same principles as stated in section 6. These are essential services without which the provision of the operator’s service to the end customer would not be possible. Particularly, in these cases no decisional authority exists vis-à-vis the contracting partner, resp. there are only very limited choices regarding the contracting partner. No processing of data beyond the purpose of performing the ISP-service takes place by the performer of the ISP-service in its own interest. In these cases as well, the operator holding the end customer relation shall be controller for data protection vis-à-vis the end customer. The performer of the ISP-service in turn shall be solely responsible for compliance with the statutory data protection- and data security provisions.

11. The demander shall be solely responsible for granting the rights of the data subjects in the scope of his own end user contractual relationship. In so doing, the undersigned operators ensure that the data subjects have one specific point of contact for the protection and enforcement of their rights vis-à-vis their direct contracting partner. Furthermore, only the demander as the direct contractual partner of the data subject is able to perform a sufficient identification of the data subject in terms of Art 11 paragraph 2 GDPR, ensuring that the end user exercises his rights exclusively with respect to his/her own personal data.

Exemplary enumeration and description of ISP-services

- **Interconnection** according to section 3 subparagraph 25 TKG (Austrian Telecommunications Act) is the physical and logical connection of public communication networks which are being used by the same or by another operator to facilitate the users of a company the communication with users of the same company or the access to the services offered by another company. Services may be performed by the operators involved or by other operators who have access to the network. Interconnection is a special case of access and is being established between the operators of public networks.
According to section 48 TKG 2003 every operator of a public communication network is obliged to offer interconnection to other operators of such networks upon their request. The extent of interconnection is stipulated in section 49 TKG 2003 (Austrian Telecommunications Act). To this extent, additionally to the master data of the contracting partner the necessary traffic data (operating data of the respective connection or routing data in case of package-oriented services to the interconnecting operator; delivery-/connection data; billing data) are being processed.

In order to facilitate the transfer of phone numbers (porting), master- and billing data are being processed in accordance with the provisions of the Communication Parameter-, Fee-, and value-added Services Regulation 2009 (KEM-V) as well as in accordance with the Number Porting Regulation 2012.

- **IP-Peering** is a connection service on the basis of an agreement (“peering agreement”) with which two ISPs connect their communication networks for the purpose of data exchange, but without charging any costs to each other. Hereby the end users of one ISP shall be provided access to the services of the other ISP. In the same way as with interconnection, the master data of the contracting partner as well as the necessary traffic data (routing data) are being transferred to the connected operator.

- **IP-Transit** designates a service whereby the data traffic is being conducted through the own network against costs. The contracting partners are usually of a different size with the bigger operator providing the smaller operator a so-called “uplink” against costs. Billing is made on the basis of the conducted data quantity. For this purpose, the master data of the contracting partners as well as the routing resp. the billing data are being processed.

- **National Roaming** means that the mobile phone of the end customer nationally uses another network than the one of the operator with whom the data subject has concluded a contract on mobile phone services. In order to be able to perform the service, no data are being processed which enable a direct identification of the data subject, but only the MSISDN (Mobile Subscriber Integrated Services Digital Network Number).

- **Leased lines** according to section 3 subparagraph 12 TKG 2003 (Austrian Telecommunications Act) are institutions providing a transparent transfer capacity between the network terminations, but with no interposition functions, which the user may himself steer as a component of the leased line offer (on-demand switching).

Leased lines particularly include
- the provision of lines with traditional interfaces (services without interposition function providing transparent transfer capacity between network terminations (symmetrically bi-directional))
- Ethernet services (services providing a guaranteed bandwidth between two network terminations)
- Blank glass fibre (= a pair of glass fibres which is being leased blank)

Summarized, leased lines are a physical connection between two points. Thus, for the performance of the services the processing of location-specific information (location data) as well as of billing data is necessary.

- **Unbundling** designates an access obligation which may be imposed on market-dominant enterprises with extensive market power according to section 37 paragraph 2, section 41 paragraph 2 subparagraph 1 TKG 2003 (Austrian Telecommunications Act) and within the scope of which a company with extensive market power shall make available line segments of its fixed communication network which lead from the switching centre to the user (or certain partial sections thereof) to other operators either physically or virtually with costs. Unbundling as an access obligation has been ordered by the Austrian regulatory authority and is available on the market as a standard offer in the form of the Agreement regarding access to the user connection line as well as the Agreement regarding virtual unbundling

In their execution basically two separate agreement relations exist: one between the access-obligated operator and the demander and one between the demander and his end customer. For the performance of the contractual relationship between the operator and the demander (e.g. creation, interference suppression) according to the respective standard offer the processing of the master data of the demander, the processing of the end customer contact information and the location-related data of the end customer are necessary.

- **Mobile Virtual Network Operators (MVNOs)** are mobile operators who do not possess their own infrastructure, but who may however offer communication services on the basis of a cooperation agreement with a mobile operator via his infrastructure.
Mobile operators with extensive market power may be imposed respective access obligations by the regulatory authority according to section 41 TKG (Austrian Telecommunications Act). The provision of services of the MVNO within the network of the obligated operator is performed with the help of the MSISDN, the Mobile Subscriber Integrated Services Digital Network Number. Additionally, the operator also receives location data of the end customer of the MVNO. Data which would allow a direct identification of the data subject are not transmitted.

II. Right to information

1. For the purpose of a transparent data processing, the undersigned ISPs will provide an insight to their customers into the concerned data processing procedures, but due to sector-specific rules they are subject to certain restrictions.

2. The provision and transmission of traffic data is done exclusively under the special conditions of the material law. Traffic data may thus according to section 99 TKG (Austrian Telecommunications Act) not be stored or transferred by the ISP, except in the cases stipulated in this provision. The right to information on stored traffic data shall therefore be fulfilled only and exclusively by the transfer of the itemized call-list (EGN) according to section 101 TKG (Austrian Telecommunications Act) to the customer.1

3. The undersigned companies may under reference to Art 15 paragraph 1 subparagraph c) provide information to recipients or categories of recipients of personal data. The latter may be particularly necessary if it concerns recipients who are doing business in the technical performance of a communication service. Severe security concerns may exist regarding a provision of information on the entirety of individual recipients – particularly in the stated area. The reason is that respective information would easily enable criminals to identify potential weak points in order to get access to the network. This may affect, resp. even endanger the integrity of the system which the operator is obliged to warrant according to section 16a TKG (Austrian Telecommunications Act).

4. Not included however is any information on data transfers to authorities within the scope of their supervisory task as well as to law enforcement agencies, to whom personal data must be disclosed for example in the context of legal interception.

5. If the data subject places his/her request for information electronically, the ISP will upon such request equally provide the information in an electronic format. The undersigned companies thereby take appropriate data security measures to guarantee a secure transfer of the data to the data subject. The provision of the information in paper is done via registered letter.

6. In order to guarantee that the entitled data subject receives the requested data, the undersigned companies carry out identity checks.

III. Right to restriction of processing

1. The right to restriction of processing of personal data shall principally serve a preliminary balance between the interest of the data subject in his/her personal data and the interest of the controller for the processing of such data. The data subject may hereby - amongst others - demand from the controller to not further process data - and equally not to delete them - because he/she requires them for the enforcement or the execution of, resp. the defence against legal claims.

2. Insofar as the data subject in the execution of this right requires the ISP to not further process, resp. not to delete traffic data, this right is contradicted by section 99 TKG (Austrian Telecommunications Act) applying to operators as a lex specialis. Traffic data may thus only be processed in the cases stipulated in the TKG. Upon termination of the connection as well as payment of the invoice, the operator must erase or anonymize the traffic data. Due to this obli-
gation the undersigned ISPs are by law not allowed to store traffic data based on the execution of the right to restriction of the processing for a period beyond such date.

3. According to section 100 paragraph 3 TKG (Austrian Telecommunications Act) as well as to the jurisprudence of the data protection authority, traffic data are provided to the customer exclusively in the form of an abbreviated itemized call-list, except if the user has declared in writing that he/she has informed all existing co-users of the line, resp. that he/she will inform future co-users, that he/she receives an unabbreviated itemized call-list. Any further going storage of passive user numbers or other information for the identification of the recipient of a message for the purpose of the enforcement, execution or defence of legal claims may therefore not be requested by the data subject.

4. According to section 101 TKG (Austrian Telecommunications Act) content data may not be stored by the ISP, a restriction of the processing is thus not possible.

5. In order to guarantee that the requesting person and the data subject are actually the same, the undersigned ISPs carry out identity checks.

### IV. Right to data portability

1. The undersigned companies understand the right to data portability exclusively in relation to personal data which have been obtained directly from the data subject on the basis of an existing contractual relationship or on the basis of a rightful consent and insofar as the processing is done with the help of automated processes.

2. Target is to facilitate to the customers the frictionless entrainment of their personal data. The undersigned companies thus offer to the data subject the personal data made available by him-/herself within the scope of the use of an ISP-service.

3. The undersigned companies comply with the right for data portability by the provision of the following personal data, such as in particular:

   a) Master data according to section 92 paragraph 3 subparagraph 3 TKG, provided by the data subject with the registration resp. during the upright contractual relationship:
      1) Name (surname and first name),
      2) Academic degree,
      3) Address (physical address)
      4) User number and other contact details for the message

Data on creditworthiness, information on type and content of the contractual relationship as well as profiling data are not included in the claim for data portability, because these are not obtained from the data subject and the interpretation of the credit assessment must be left to each controller, in order to guarantee a fair competition.
b) Other data made available by the data subject, such as in particular:
1) Date of birth
2) E-Mail-address disclosed by the data subject
3) Content of the E-mail-inbox (if the operator is also the E-mail-service operator of the inbox)
4) Bank details

4. In terms of due process, it is however excluded from the right to data portability that traffic data or unabbreviated itemized call-lists (EGN) are transmitted as these are not obtained directly from the data subject and data protection rights of third parties would be directly affected. Furthermore, according to section 99 TKG (Austrian Telecommunications Act) traffic data may not be stored or transmitted by the ISP except in the cases expressly stipulated there. The transfer of stored traffic data to customers is thus permitted exclusively within the scope of the itemized call-list (section 100 TKG). According to the jurisprudence of the data protection authority no further going traffic data are being disclosed to the customer and therefore they are ported neither.

Provision of data to the data subject
5. The undersigned companies provide the personal data to a data subject, which he/she has directly provided based on a rightful consent or within the scope of a contractual relationship, in electronic form (e.g. as download or transmission via E-Mail).

6. In order to facilitate the provision via download, the data subject is either transmitted a download link or a download button is being installed in the customer area on the company website.

7. Data which may be obtained by the data subject him-/herself at any time in a current machine-readable format, shall be deemed made available.

8. The undersigned companies refrain from any kind of technical measures which would impede a later transfer of data obtained from the data subject to a new controller.

File format
9. Master data of the data subject in terms of item 3 a) 1 - 4 as well as date of birth, E-Mail-address and bank details are being collected by the undersigned companies and provided as a text file in a common format, for example in XML, CSV or XLS format.

10. The content of the E-Mail-inbox is provided in a common format such as for example the MBOX-file-format or by retrieval possibility via IMAP, POP or ActiveSync.

11. It is at the discretion of the operator whether he ports individual data or data categories, resp. all data collected in one file (e.g. ZIP-file) as an archive.

Provision of the data to a new controller
12. If the data subject so wishes, the undersigned companies - unless stated otherwise - provide the registered data to the new controller in the same way and manner as to the data subject.

13. In order to ensure the implementation of the provided data by a new controller, common technical standards are required within the ISP-industry on the European level. Until then the further usability of the data by the new controller may possibly not be guaranteed.

V. Proof of identity

In order to guarantee that the entitled data subjects exercise their rights as data subjects according to the GDPR, the undersigned companies may carry out identity checks.
VI. Data-Breach-Notification

1. In case of a security event leading to the violation of the protection of personal data, the undersigned companies will immediately, at the latest however within 24h, deliver a notification to the Data Protection Authority (Data-Breach-Notification).

2. The undersigned ISPs meet the formal and content requirements for the notification within the scope of the Data Breach Notification, which are specified in detail in the sample form (Annex A).

3. If the ISP omits a notification, he shall state the reasons therefore within the scope of his duty to documentation.

Notification of the data subject

4. Insofar as the violation of the protection of personal data likely leads to a material or immaterial damage for the data subject, the ISP in addition to item 1 transmits a notification to the data subject. The higher the potential damage, the lower the necessary probability of occurrence to induce a notification.

5. Due to the fact that the ISP can only contact his own contracting customer, but not any other possible conversation partners who may equally be affected by the Data-Breach, it is only possible for the undersigned ISPs to transmit a Data-Breach-Notification to the respective contractual customer. Insofar as a high number of non-contractual customers is affected by the Data-Breach, the ISP will inform these of the Data-Breach via a public notice.

Evaluation criteria

6. The undersigned ISPs evaluate the imminent severity of damage as well as the probability of its occurrence on a case by case basis by means of the type of the security event, the categories of the affected data as well as by means of the resulting possibilities of misuse by third parties.

7. It is particularly taken into consideration whether one of the following scenarios is imminent:
   a. loss of control over the data,
   b. discrimination,
   c. identity theft or - fraud,
   d. financial losses,
   e. unauthorized clearing of the pseudonymization,
   f. harm to someone’s reputation
   g. loss of confidentiality of data subject
to professional secrecy

8. The probability of damage occurrence may be appropriately lowered by technical and organizational measures which the ISP has taken or will take in relation to the affected personal data.

9. A high risk for material and immaterial damages for the data subject is being assumed by the undersigned companies particularly if unabbreviated credit card numbers, passwords or communication content are affected.

VII. Participation in the Code of Conduct

1. Internet Service Providers who fall under the territorial and material scope of application of this code of conduct, may subject to them and shall announce it via E-Mail to aufsichtsbeirat_coc@ispa.at or by mail to Währinger Strasse 3/18, 1090 Vienna.

2. If the prerequisites according to item 1 are not given, the concerned applicant shall not be included in the list of undersigned companies.

3. A current list of all companies who have subjected to the Code of Conduct for ISPs shall be published on the ISPA website. This list shall include the name and address of the undersigned company.

4. The undersigned companies shall put a link on their websites to the current list of undersigned companies.
VIII. Monitoring of the Code of Conduct

1. A supervisory board is set up as an organizational unit within ISPA and serves as the body responsible for monitoring compliance with this Code of Conduct in accordance with Article 41 GDPR.

2. Each signee of this Code of Conduct recognizes the recommendations and decisions of this supervisory board.

3. The exact criteria for appointing the members of the supervisory board as well as its concrete competencies are set out in separate by-laws. These can be found at www.ispa.at/coc.
Annex A

I. Sample Form for a Data-Breach-Notification to the Data Protection Authority on a violation of the protection of personal data

(Any information should as far as possible be already included in the first notification to the authority, which shall be made without delay, no later than 24 hours as of the detection of the event)

Remark: the present form corresponds to ANNEX I of the (EU) Regulation Nr. 611/2013 of the Commission dated June 24, 2013 on the measures for a notification on violations of the protection of personal data according to the directive 2002/58/EG of the European Parliament and the Council (Data Protection Regulation for electronic communication) as well as to the requirements of section 95a TKG. This form also considers the minimum requirements of content for a notification according to Art 33 Regulation (EU) 2016/679 (General Data Protection Regulation).

Information regarding the operator

1. Name and contact details of one or several contact persons for possible enquiries

Name: ____________________________  Position: ____________________________
Telephone number: ____________________________  E-Mail-Address: ____________________________

2. Statement whether it is a first notification or a subsequent notification

☐ First notification  ☐ Second or subsequent notification

3. Date and time of the event (if known, may be estimated if necessary) and of the determination of the event

Date and time of the event: ____________________________  Date and time of the determination of the event: ____________________________

4. Type of violation of the protection of personal data

☐ Destruction, loss, damaging, unauthorized disclosure
  ☐ Destruction: The data are no longer available/have been deleted
  ☐ Loss: The data still exist, but the controller has lost control/access/possession
  ☐ Damaging: The data have been modified, damaged or are no longer complete
  ☐ Unauthorized disclosure: Transfer of data to recipients who are not entitled to receive the data (or to access them)

5. Type and content of the concerned personal data sets

Description of the concerned data categories and the approximate number of concerned personal data sets (particularly whether special personal data are concerned, data on criminal convictions, biometric data or health data)
6. Categories and number of data subjects
Indication of the potentially concerned groups summarized according to typecast indications ("employees", "customers", ...)

If an indication of the number is not possible, a justification why an estimation of the number of concerned users or persons is not possible at the time of the notification.

7. Technical and organizational measures which the operator has taken with regard to the concerned personal data (or which he is going to take)

Technical and organizational measures in order to eliminate the occurred violation as well as to minimize the detrimental effects if appropriate e.g. resetting of passwords, access blocking, reporting to the competent police office in case of criminal actions

8. Possible consequences and possible detrimental effects on participants or data subjects

Information on the potential material or immaterial damages, such as loss of control over the personal data, discrimination, identity theft or - fraud, financial losses, unauthorized clearing of the pseudonymization, damaging of someone’s reputation or the loss of confidentiality of data which are subject to professional secrecy
II. Sample Form for a Data-Breach-Notification to the data subject affected by the violation of the protection of personal data

(The information has to be provided in clear and plain language)

Remark: the present form corresponds to the minimum content requirements for a notification according to Art 34 of the regulation (EU) 2016/679 (General Data Protection Regulation).

Exclusions from the notification obligation (if the operator omits a notification, he shall state the reasons within the scope of his documentation duty).

1. Existence of technical and organizational security measures which are appropriate to make personal data inaccessible to unauthorized persons (encryption, pseudonymization)
2. Measures taken subsequent to the data protection violation which eliminate the originally high risk of a damage
3. The notification would constitute an inappropriate effort (in such case only a public notice shall be made)

Information regarding the operator

1. Name and contact details of one or several contact persons for possible enquiries

Name: __________________________ Position: __________________________

Telephone number: __________________________ E-Mail-Address: __________________________

2. Date and time of the event (if known, may be estimated if necessary) and of the determination of the event

Date and time of the event: __________________________

Date and time of the determination of the event: __________________________

3. Description of the type of violation of the protection of personal data

Destruction, loss, modification, unauthorized disclosure

☐ Destruction: The data are no longer available/have been deleted
☐ Loss: The data still exist, but the controller has lost control/access/possession
☐ Damaging: The data have been modified, damaged or are no longer complete
☐ Unauthorized disclosure: Transfer of data to recipients who are not entitled to receive the data (or to access them)

4. Technical and organizational measures which the operator has taken with regard to the concerned personal data (or which he is going to take)

Technical and organizational measures in order to eliminate the occurred violation as well as to minimize the detrimental effects if appropriate

E.g. resetting of passwords, access blocking, recording with the competent police office in case of criminal actions
5. Possible consequences and possible detrimental effects for the data subject

Information on the potential material or immaterial damages, such as loss of control over the personal data, discrimination, identity theft or fraud, financial losses, unauthorized clearing of the pseudonymization, damaging of someone's reputation or the loss of confidentiality of data which are subject to professional secrecy.

Version
Version 1.1. v. 16.06.2020

About ISPA
ISPA Austria is the voice of the Austrian Internet industry founded in 1997 as a non-profit association which represents the interests of more than 200 members from all sectors around the Internet industry as a voluntary interest group. Our goal is to shape the economic and legal framework supporting the optimal development of the Internet and Internet services. We regard the use of the Internet as an important social skill and acknowledge the resulting socio-political responsibilities.