**Austrian Federal Chamber of Labour**
**Department of Consumer Policy**

# Digital User Rights

## With a Focus on Data Protection

8/2014

# Digital User Rights

**Digitalisation technology in general and the Internet in particular are changing the foundation and playing rules of entire sectors and facets of life. New technologies and forms of service are penetrating ever more deeply into our everyday lives at work and as consumers, our social life and our leisure time behaviour. Technology advances cost jobs and create new ones. We are faced privately and professionally with the pleasant as well as the undesirable aspects accompanying digital development and life in an information society. We have reconciled ourselves to a certain degree with grey zones and rule breaking on the Internet. However, that should not curb our commitment to finding effective concepts for making and enforcing laws for the digital world despite all these difficulties. The following list contains the chief goals but has no claim to completeness:**

**Data Protection**

- **Top priority:** The challenge of ensuring the protection of fundamental rights even in the digital age is being accepted more proactively. These rights include the right to privacy, data protection and freedom of information but also general protection of digital users from being defrauded. The EU Commission and EU Parliament intervene to protect against and correct power imbalances and dangers undermining the rights of digital users. Internet regulation and the field of action of technology design are not left just to companies and their engineers. Who profits from the digital revolution? To ensure that “all of us” can be the answer to this question, digital users’ rights in general and data protection in particular are given top priority in European policy.

- **Consumer protection to ensure freedom:** Protection of personal data and respect of private life are rights that are anchored in the Charter of Fundamental Rights of the European Union. As such, they have finally attained the status they warrant in a society based on civil rights and liberties. All individuals have the right to determine themselves how their own personal data is used. This right is defended against restrictions motivated by economic and regulatory factors and expanded in a contemporary manner. Consumer protection advocates also seek to ensure fundamental liberties.

- **Transparency:** Data processing procedures often occur unnoticed by the affected individuals and must be rendered more transparent. Transparency is also called for in other contexts, e.g. in connection with the criteria for the order in which search machine results are listed, with evaluation platforms where it is unclear whether the product recommendations were manipulated or with Internet contents whose lack of designation means they can be editorials or simply advertising.

- **Clear dos and don’ts**: Legal certainty is improving on the question of whether a certain type of data use is admissible or inadmissible in different use contexts in the digital world**.** This improvement entails clearly defined limits of admissibility for data processing and processing prohibitions. The only exception should involve the weighing of individual cases to determine whether interests of confidentiality or use predominate for the given data. In the event of a dispute, the courts and the data protection authorities must decide.

- **Strict rules for trade in data instead of tales of “voluntary” approvals:** Trade in digital data is characterised by a lack of transparency and a great imbalance of power and requires a realignment of the law. Against this backdrop, a person’s consent to the use of his or her personal data is an unsuitable basis for the admissibility of data processing in most cases. User protection is therefore being stepped up by putting in place legal restrictions on data use.

- **Data economy:** The principle of data economy is being pushed on all levels. Not all uses of data aimed at justified goals are legitimised by an overriding public interest. Obtaining consent from the individuals involved should not provide the necessary legitimacy for every use of data. Typically, there is a considerable imbalance of power among the parties involved. Consent is anything but voluntary. Other fundamental rights such as the right to information and property must also be respected. However, the principle of data economy in particular needs to be strengthened, so it does not fall far behind.

- **Preventive data protection** – or advance checks by the authorities or a push for the acquisition of data protection quality marks. The subsequent determination of data protection violations and losses is not an equivalent substitute for the precautionary prevention of same. These efforts include preventive protection against misuse by setting sector-specific data protection duties that are as concrete as possible. In data protection, cutbacks should not be permitted even in individual cases incurring considerable costs.

- **Internet corporations under close scrutiny:** Efforts are being intensified at EU level to enforce user rights in connection with Internet corporations that have their registered office in non-EU countries, particularly the United States. Quasi monopolies such as Google, Apple, Facebook, Amazon, inter alia have virtually unlimited market power, global presence and a gigantic volume of customer data. The EU Commission must be persistently reminded that competition is being distorted by these types of over-the-top players who do not abide by EU rules pertaining to European users of their services. The EU Commission is pushing for further supervisory processes and informal settlement solutions. Its aim is to have global corporations take responsibility in conformance with EU law on consumers and data protection.

- **Noticeable sanctions** should be levied against systematic breaches of data protection. Currently, data users do not have to reckon either with a (quick) uncovering of illegal uses of data nor with punishments that would deter them. As a rule, investigations are only launched in response to massive complaints or media coverage. It is extremely rare for (appreciable) penalties to be imposed. The effectiveness of supervision and sanctions must be increased dramatically.

- **A powerful supervisory authority:** The data protection authorities must have the resources and technical expertise to keep pace with the tough requirements of a supervisory authority of this kind. Given the millions of data processing operations, national authorities need support to maintain an overview of the market. This support includes operational data protection officers at all companies if possible.

- **Governmental sovereignty instead of everyone being a plaything of the secret services:**
  The revelations of the former US secret service employee Edward Snowden brought to light the excessive spy activities of the NSA and associated services. There must be consequences for these excesses. The most urgent questions on the precise scope of data protection violations by the secret services in telecommunication networks are quick to clarify. Operators of large Internet exchange servers must be made to discharge their duties under data protection law more effectively.

- **Greater protection from Internet crime:** Internet crime is on the rise, be it in the form of fake shops, phishing e-mails, identity theft or hacking. What are needed are focused interdisciplinary campaigns, focused public prosecutors' offices for cybercrime, a more precise determination of the level of online fraud and improved structures for cross-border collaboration in order to reduce the enormous shortcomings in enforcement (majority of proceedings are quashed).

- **Regulation of special digital issues**: Digital issues did not exist to the current extent or at all when the data protection directive was first passed in 1995. These issues include everyday phenomena such as always-on (mobile) broadband Internet service, big data analytics, scoring and profiling, digital market research through individual tracking, behaviour-based online advertising, data saving in clouds, cybercrime, Web 2.0, network conflicts between freedom of information and data protection, plus many more. Issue-specific data protection regulations must therefore supplement the general principles. This step will render the general stipulations for the given scope of use more precise.

- **Requirement to anonymise:** In the enforcement of data protection law, anonymising is being pushed as an expression of data economy. Prior to use, data must be fully anonymised if the need for a personal reference is not clearly proven. The use of pseudonyms should be the exception because data users can restore the personal reference to themselves again in this case.

- **Tougher requirements on consent to data use:** Approvals in the form of implicit acceptance of business conditions (not read) must become a practice of the past. The user of the data must in any case seek to obtain an active, explicit signal from the individuals involved, in other words, have them click a box to put a checkmark in it on the Internet or obtain a signature from them.

- **Greater protection against direct marketing**: Direct marketing must not be allowed to be privileged by being subject merely to an opt-out rule. This would fall far short of keeping the promise to provide contemporary data protection on the Internet. Consumers expect the data user to obtain their explicit consent to the use of their data for marketing purposes (opt-in rule).

- **Data use only within the scope of the original purpose:** Data is not allowed to be used for purposes not in harmony with the purpose for which it was originally saved. Exceptions to this prohibition (such as processing for statistical or historical purposes) must be handled restrictively and listed fully.

- **Extension of EU data protection to non-EU countries:** It is important that the applicability of the future data protection regulation be extended to non-EU countries such as the United States, for example. At the same time, enforcement agreements and assistance with legal remedies must be pushed; otherwise, pending legal claims from European citizens will continue to be difficult to enforce.

- **Automatic information for consumers:** Individuals affected by data processing operations must obtain more information from the data users before data is compiled. Consumers must be told in advance the name and contact details of the party responsible for the data, the purposes of data use, the concrete duration of storage, the origin of the data, whether the provision of data is required or voluntary and the like.

- **Strict duty to provide information about data origin and recipients:** The duty to provide information regarding the origin of the data refers only to “available data”. Data users are currently required to provide information only about “recipients or recipient groups”. They satisfy the obligation merely by divulging the sector (e.g. financial service provider). In future, the companies must also be named, so the affected individuals can exercise their rights in the first place.

- **Special deletion rights on the Internet:** Facebook users post massive amounts of personal data about themselves and others. There should therefore be a right to the complete deletion of self-generated content on the Internet. It would also be an improvement if the party who posted personal data on the Internet were obligated, wherever possible, to inform third parties who further processed this data that the Internet user requested the deletion of all cross-references and copies.

- **Clear limits for profiling and personal assessment:** The proposals from the EU Commission, EU Parliament and Council create broad permission for businesses interested in profiling. Data protection and legal protection concerns of consumers come off badly in the process. Crucial questions such as the following are neglected: What requirements have to be met for personal profiles to be drawn up in the first place? Which types of data are allowed to be processed at the outmost?

- **Cessation of illegal tracking methods:** Regulation of the use of technical tools employed for tracking user conduct on the Internet must be effective and reflect actual practice. The efforts to curb illegal spying of surfing behaviour must be stepped up. For instance, restrictive rules are needed for the use of "Deep Package Inspection", a process with which data packages on the Internet are monitored and filtered.

**Limits to the use of big data analytics and forecasts**: These procedures work with classifications (e.g. assignment to credit rating classes), clusters (e.g., defining a customer group with a propensity to switch providers) and forecasts (future-orientated behavioural assumptions). Data analyses are done, for instance, to weed out undesirable customers. Action is needed. Valid data protection regulations must also be effectively enforced in the field of data-based forecasting. Conventional data protection must be supplemented by adding a prohibition of discrimination by means of assessment processes. Legal loopholes with respect to the binding purpose of a data processing operation must be closed.

- **Rules for scoring:** Credit ratings based on largely automated scoring procedures increasingly decide whether consumers are accepted as contracting parties. Clearly, loans cannot be extended without some kind of check. However, the scope of regulation is currently meagre. There is an urgent need for a scoring law with rules on execution that limit excessive scoring. Affected individuals are not allowed, for example, to be subject to arbitrary and discriminatory behavioural designations.

- **Greater personal responsibility on the part of data processors**: The EU Commission would like to make data users take on greater responsibility – in the form of obligatory sets of documentation, safety measures, data protection officers and risk assessment for applications involving sensitive data. Although this step would privatise the tasks of the authorities, data protection authorities would clearly be unable to keep an eye on millions of data applications at the same time. Data processors should have sensitive projects (as defined by the data protection authorities) checked at their own expense by independent boards of control to achieve conformity in data protection and then present the results to the data protection authorities.

- **Retain the register of residents:** The register of residents meets an important publicity purpose (everyone can examine it) and gives data protection authorities insight into the actual practices of data processing. Considerable penalties should be imposed on data users for not registering.

- **Privacy by design and default:** Data protection must be planned during the actual development of new technologies. The EU Commission's proposal on this issue is too non-binding to be beneficial in actual practice. Concrete specifications must be laid out. For example, there should be binding requirements for online services to make privacy settings as strict as possible.

- **Mandatory operational data protection officer:** The introduction of a mandatory operational data protection officer in the private sector must be a core element in any serious reform of data protection. The free flow of data within the EU suggests that standard EU-wide regulation would be the way to go. The goal is the mandatory use of an officer in as many enterprises as possible (e.g. all companies with more than 20 employees).

- **Mandatory technical inspection associations for data protection:** Soft promotion of data protection quality marks falls short of what is needed. Certification must be a mandatory standard for applications involving sensitive data. Without this step, data protection regulations would not meet the demands of the 21st century.

- **Exceptionless obligation to report serious data mishaps:** A full reporting obligation should be a matter of course. It would enable the data protection authorities to initiate an examination procedure quickly through official channels, thereby protecting affected individuals from further damage.

- **Competence of authorities but without a one-stop shop**: Giving exclusive competence to local data protection authorities at the company's principal place of business would greatly impede access to the law for affected individuals. This approach incites corporate groups to establish themselves in places where the enforcement of data protection is especially weak. In the event of group-wide data applications, national data protection authorities should therefore be not only the first place for affected individuals to contact but should also have authority to make decisions.

- **Data protection authorities as "consultants":** Apart from formal official decisions, the dialog between data processors and their supervisory authority must be intensified. In a sector often dominated by small enterprises, a low threshold for obtaining expertise is important to prevent businesses from failing to comply with many data protection regulations because of ignorance or being overwhelmed.

- **Effective enforcement of the law:** Official advance checks are needed to minimise the risk of uses involving sensitive data. Along with the right to represent clients in procedures involving protection law, institutions that safeguard the interests of consumers should be given the right to institute legal actions as an association.

- **Rule violations and shortcomings in enforcement:** Rule violations on the Internet are in some cases overwhelming governments based on the rule of law. Government control bodies, data protectors and consumer advocates can do little to counter the multitude of actions on the Internet that warrant prosecution. The resources and work methods of the authorities and the justice system do not meet the requirements of the digital age and must be massively expanded. The objective is to conduct investigations even in small-scale cases (e.g. dispersed damage with a big number of affected individuals) and especially large-scale cases (e.g. Internet corporations, secret services).

- **Administrative punishments as deterrents**: It is important to have threats of punishment that serve as deterrents. They also have to be enforced, however. If the authorities hardly exercise their penal power because of underfinancing, for example, the effectiveness of the threat of punishment – even severe punishment – will remain minimal in actual practice.

- **Collaboration of national and EU institutions:** Data protection authorities, the EU Commission and consumer associations need to act in concert with each other. That way, they can create the bargaining power required to influence the marketing practices of international Internet corporations in ways that benefit the rights and needs of digital users. This collaboration must be institutionalised. Settlements should not be allowed to keep the member states from clarifying individual legal issues through legal proceedings.

- **Relief for consumer organisations:** Injunctions in one country do not prevent providers from relying on the same dubious business practices elsewhere owing to the territorial effect of court decisions. One should consider the extent to which parallel decisions in other member states could be facilitated in the spirit of procedural economy. An EU-wide company register and a reform of connections in line with the E-Commerce Directive are overdue.

- **Data transmissions outside the EU:** The United States is the most important data recipient in the exchange of data with Europe and also verifiably commits systematic data protection violations. The Safe Harbour Agreement between the EU and the US has proven worthless in actual practice. The EU now has no choice but to cut down on data transfers in countries that lack an equivalent level of data protection.

- **TTIP – priority for strict data protection:** As part of TTIP negotiations on a free trade agreement between the EU and the US, the EU must not be allowed to shy away from a conflict between different data protection traditions. It must ensure that EU data protection regulations are not undermined and that they can be further developed.

**Additional rights for digital users:**

- **Requests for reasonable blocks of automatic access to websites by search engines**: The EU Court of Justice ruled in 2014 that Google is obligated to delete search findings at the request of an individual involved. The EU Court of Justice was criticised for favouring censorship because of this ruling. Clarification is needed at EU level regarding the criteria for carrying out or rejecting a deletion, among other matters.

- **Transparent and fair search engine rankings:** With over one billion visitors a month, Google tries to give the impression that the order in which the results appear is determined by means of incorruptible search algorithms. A broad discussion needs to be conducted on the factors that search engines use to rank a website in a transparent and competitively neutral manner. Techniques that go beyond an optimisation of the search engine and manipulate ranking results must be actively repressed.

- **Data protection specifications for the use of social networks:** Operators must be emphatically requested to offer settings that protect privacy, to pre-set them at strict levels and to abide reliably by data protection provisions. Most platforms finance themselves through targeted advertising. This business model is difficult to reconcile with the idea of data economy. One must at least put in place provisions requiring, inter alia, that data releases be checked by the users personally and that user data be completely deleted physically after voluntary consents are cancelled or the use of the service ends. In case of misuse (e.g. identity theft), the operator must respond quickly to blocking notifications.

- **Data protection rules for geo-based services:** Smartphone users can be identified by means of UDID/IMEI, phone number, time-route profiles, various login data, and much more. Users need greater protection against the analysis and exploitation of their geo-data (location, speed of movement, and the like) through restrictive legal provisions. Surveillance fantasies on a new scale (e.g. car insurance companies monitoring the driving behaviour of car drivers) must be rejected. Access to geo-data should be rendered easily detectable by means of pictograms on the display. More finely graduated forms of consent regarding access to data are also required.

- **Minimal harmonisation for further sectors or technologies sensitive to data protection:** Nearly every technical application that can be used to collect personal data raises urgent issues and concerns regarding the confidentiality and security of the data. The abstract data protection and security regulations must be rendered more precise, e.g., for the use of radio frequency identification (RFID), biometrics, electronic wallets, computer-dominated cars (aka “connected cars”), smart meters and public digital applications that are sensitive with regard to data protection.

- **Online advertising:** One of the most elementary principles of advertising is that it must be clearly perceived as such. It is not allowed to violate the right to privacy. It is not allowed to apply (in)direct pressure on minors to make a purchase. These principles have little weight on the Internet. Consumers are often misled and guided into cost traps with advertising reward systems in games, advertising in apps and in-app purchases. The enforcement of existing laws must be improved, so advertising and sponsoring are also transparent in the digital world, children are not taken advantage of and no illegal behavioural profiles are created.

- **Fair user rights with respect to copyrighted digital goods**: Adjustments to copyright law in the digital world primarily benefit the position of the holders of rights. New dependencies are created in the process: Providers use technical barriers and licence conditions to determine unilaterally and to their own benefit what users can and cannot do with digitally acquired contents. That is why consumer rights now have to be strengthened**,** say, by concretely enforceable free usufructuary rights such as digital private copies, a truly free internal market and specific minimum contents for contracts on the retrieval of digital goods.

- **Guarantees of legal protection for the enforcement of intellectual property rights:** Several measures of this type are suitable for impairing users’ privacy and freedom of information. Extrajudicial encroachments on user rights should not be allowed. For instance, Internet providers cannot decide themselves on the passing on of data, filter actions or the blocking of customers. All encroachments on the fundamental rights of Internet users must therefore be subject to judicial review. Moreover, Internet users need protection from a “reminder industry” that pursues private Internet users with excessive demands for payment due to actual or alleged violations of law.

- **Internet neutrality:** Concern about the waning significance of “Internet neutrality” also shows that laissez faire is no option for action. The goal is to put in place a legal framework that prevents the Internet from disintegrating into various underclasses dependent on the solvency of the service providers and users. There is a need for regulatory actions to meet user expectations that transported data packages will be treated (largely) equally. These actions concern the transparency of the acquired service, respect of fundamental rights, diversity of offerings, freedom of choice, quality of services, the fight against unfair competition and the promotion of innovative services.

- **Market concentration:** Global corporations such as Google, Amazon and Facebook have a market power against which national governments and EU institutions provide too little counterbalance. A priority objective of the EU Commission should be to enforce fair competition on the Internet by means of (further) supervisory processes. The purpose of promoting innovation is to support open-source and free software that enables others to make advances.

- **Participation processes concerning topics with great social ramifications:** Certain trends in the digital world affect practically everyone, whether they involve private video surveillance with cheap video cameras from DIY warehouses or electronic patient files or digital electricity meters for all households. More frequent use should be made of participation models to allow affected citizens to be well integrated in terms of information, to address concerns and anxieties, and to investigate undesired consequences or alternatives thoroughly.

- **Media competence and risk awareness** regarding risks on the Internet must be conveyed in connection with education in schools and public education efforts. Data protection officers at companies – if made mandatory – would be enormously important informational hubs for passing knowledge onto employees and for initiating critical discussions on risky technologies in their environment.

- **Minimum harmonisation for further sectors or technologies:** Nearly every technical innovation involves issues and concerns of a more or less urgent nature regarding user rights, warranties, liability, confidentiality and data security. In these kinds of sensitive areas, the general rules must be broken down into concrete exercising rules and user rights. Binding rules on the following are part of these efforts, e.g.:

    - **for the use of radio frequency identification (RFID),**
    - **for the use of biometrics,**
    - **for electronic payments,**
    - **for connected cars and**
    - **for smart meters.**

- **Risk-free age check:** Age monitoring systems on the Internet should not be allowed to entail disadvantages for young people. The providers have a duty to ensure that children and young people do not have access to content deemed age-inappropriate under the provisions of youth protection law. In addition, the providers must strive to protect minors from payment defaults on legal transactions not approved by their parents. The most common approach is to ask for the year of birth or to use clauses in general terms and conditions of business, the acceptance of which by users indicates that they are of age. Young people seldom pay attention to clauses and falsify age information, sometimes without a clue. Among adolescents 14 and older, there is always a suspicion of fraud if they use services in disregard of the age restriction and become financially overwhelmed when it comes to paying for them. Steps must be taken to ensure that age checks are conducted in a way that is sensitive to data protection and that does not criminalise young users.

- **Strengthen consumer rights in relation to copyrights:** Providers use technical barriers (digital right management (DRM) systems) and licence conditions to determine unilaterally and to their own benefit what users can and cannot do with digitally acquired contents. New dependencies arise from this situation. Online providers utilise self-contained systems sometimes consciously to bind users to them. Users are prevented from unhindered use also by contradictions between file formats and certain players. In most cases, the providers do not offer users any assurances either that the technology used will remain unchanged over time. So, pressure can very well mount on users either to accept the obliteration of their own archive, consent to software changes or purchase new terminals. Consumer contract rights and copyrights often collide with each other. For instance, licence conditions for the online purchase of music, games and the like frequently exclude any and all warranty rights with a reference to copyrights. The provider side uses contractual and technical barriers to reduce traditionally customary possibilities of use (e.g. private copies) and legal claims (e.g. warranty).

- **Actions against Internet crime**

  The frequency of fraud cases is increasing parallel to the boom in Online Shopping, Social Networks & Co. The Austrian Federal Ministry of the Interior recorded about 12,000 reported cases of cybercrime in Austria in 2014. Internet crime is on rise, be it in the form of fake shops, real estate and trust fraud through want-ad platforms, phishing e-mails, brand counterfeiters, identity theft, hacking or plundered bank accounts. With the help of the Internet, even classic offenses such as deception, extortion, money laundering or libel can be committed with comparative ease across borders and often anonymously. Every third complaint filed with the Austrian Internet Ombudsman pertains to one of the many rip-offs and cybercrimes found on the Internet. Dependence on the functionality of the Internet has grown so much that there is a need to conduct an intensive analysis of aspects such as data security on the Internet and damage that private Internet users can also suffer from hacking attacks, the spread of malware, the deliberate overloading of servers, the theft of digital identities or the manipulation of data.