ULN
UNITED LEGAL NETWORK

Law Review

Vol. 2/ 2013 ULN united.legal.network EEIG

www.united–legal–network.com

Content:

Note:

The main topic of this ULR is data protection. The French contribution has already been printed in ULR 1/ 2013 (La protection des données personelles dans l'entreprise by Leonard Goodeneogh, Paris) and has been repeated in this volume for the sake of completeness.

Beginning with Vol. 1/2013 the ULN Law is published only as digital version. If you are interested in receiving the Law Review regularly please write a short message to info@united-legal-network.com.

Why and how to care about data protection?

A real explosion of data traffic is to be exspected. Till 2016 more than one Zettabyte, which is the equvalent of 328 Billion DVDs will be transferred through global IP networks. In 2011 we had a 15% growth on internet users, in figures 2.3 billons. 58% use their smart phone for internet access.
At the moment we have 1.5 Billion active social media users. A good example is online dating. More than 30 % of all relationships in Europe are based on online dating services. In Germany more than 7 million users are registered on online dating plattforms.. About 1 millions Germans flirt mobile.

The tremendous pace of technological developments impairs appropriate legislation. There is a need for international regulation for international constellations. At the moment we have a lack of legal security, and therefore totally different interpretation by courts, whichof course results in forum shopping. Unclear or inadequate provisions lead to low level of regulation, of course there is a low acceptance and enforceability than.Offline principles can not be transferred 1:1 to the Internet and the more specific a law is, the faster it will be overtaken by technical progress.

There is a Legal Framework by the EU now, but it is by far not enough
I.Directive 95/46/EC of the European Parliament and of the Council of´24 October 1995 (the Data Protection Directive)
II.Directive 2002/58/EC on privacy and electronic communications of 12 July 2002
III.Regulation 45/2001

Because oft he lack of legal security there hast o come a General Data Protection Regulation. The first and inaugural draft was in 2012.
The key changes compared to German law are:

- A single set of rules on data protection, valid across the EU (Regulation instead of Directive)

- Right to be forgotten
- Privacy by design and default
- Requirement for explicit consent
- Right of data portability
- Data Breach Notification: Obligation to notify serious data breaches without undue delay
- Fines of up to 2% of annual worldwide turnover (Art. 79)
- General competence of only one data protection authority within the EU for each company with several establishments.
- Right to refer all cases to their home national data protection authority for individuals.
- Application of EU law for companies established in so-called "third countries", if they offer goods or services in the EU.
- Increased responsibility and accountability for those processing personal data.
- Reduction of administrative burdens such as notification requirements for companies processing personal data.
- Strengthening of national data protection authorities.
- Data Protection Officer now obligatory for entities with 250 or more employees

The EU Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE") voted on 21st October 2013 to adopt its report on the draft General Data Protection Regulation and the separate Directive for the law enforcement sector. This vote sets out the Parliament's position for its negotiations with the Council and Commission (known as the "trialogue" stage). The Committee aims to have a plenary Parliamentary vote in March before the Parliamentary elections.

The report contains significant amendments compared with the original draft prepared by the European Commission in January 2012. In the same time, the currently adopted version did not include or softened down a number of very strict provisions written into the very first draft report published by LIBE's rapporteur, Jan Philipp Albrecht, in December 2012. The following changes to the previous drafts are of particular note:

- The Parliament's draft proposes that sanctions could be as high as €100,000,000 or 5% of annual global turnover (whichever is the greater), compared with the Commission's proposal of €1,000,000 or 2% of annual global turnover.
- Compliance programs and accountability will be taken into account when applying sanctions;
- Sanctions can include the obligation to perform periodic audits;
- The conditions for consent have been tightened up. In particular, consent cannot be tied to a contract;
- "Legitimate interest" remains in the regulation as a valid basis for most kinds of processing (except for sensitive data and profiling);
- Data portability stays in the regulation, but it is merged with the article on right of access;
- the "right to be forgotten" is relabelled "right to erasure," but its provisions are for the most part unchanged;
- The rules on jurisdiction are essentially unchanged from the Commission's draft. A data controller located outside the European Union will be subject to

the regulation if the data controller "offers goods or services" to data subjects in the EU, or "monitors" them;

- The one-stop shop mechanism is maintained, except that consumers may always complain to their local DPA, instead of being obligated to go to the main DPA responsible for the controller's activities;

- A data protection officer would be obligatory for any company processing

- personal data relating to 5,000 data subjects or more during any consecutive 12-month period;

- Data breaches would have to be reported "without undue delay," with a presumption that 72 hours is "without undue delay";

- A data protection risk analysis would become obligatory for any processing involving more than 5,000 data subjects during any consecutive 12-month period, or any other kind of risky processing;

- Extensive new provisions have been inserted on data processing in the employment context;

- Transfer of personal data to countries outside the EEA is made more difficult, particularly if a proposed transfer is in response to a request from a court or an administrative authority of a third country. A firm would first have to get permission from the local DPA. This amendment is a response to the concerns triggered by the Snowden disclosures on NSA surveillance; and

- Data controllers must use standardized symbols to tell consumers how their data is handled:

The vote now permits the Parliament to proceed to the trialogue negotiation with the Council and Commission once the Council has reached an agreed position. Previously the high number of amendments (approximately 4,000) proposed by the Parliament to the legislation had given rise to concerns that the Regulation would not be passed before the next European elections. Now that the European Parliament has made its position known, pressure will shift to the Member State governments to reach agreement on a position within the European Council. Once a common position is reached, negotiations can begin with the European Parliament and Commission.

Andrea Hellmann
Munich, Germany

Google in der Schweiz zurückgebunden

Ausgangslage

Google bietet seit 2009 für die Schweiz den Dienst „Street View" an. Google „Street View" ist eine Funktion in Google Maps, mit welcher sich virtuelle Rundgänge namentlich durch Strassen und Plätze unternehmen lassen. Die Aufnahmen der Strassenbilder erfolgen jeweils mit speziell ausgerüsteten Fahrzeugen, wobei die Gesichter von Passanten und die Kennzeichen von Fahrzeugen von der Software automatisch verwischt werden. Die Erkennungsrate der Software ist jedoch nicht vollständig. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte verlangte von Google weitere Massnahmen, was Google ablehnte. So mussten die Gerichte entscheiden. Das Bundesverwaltungsgericht gab dem Eidgenössischen Datenschutz-beauftragten weitgehend Recht. Das von Google angerufene schweizerische Bundesgericht gab Google in einigen Punkten recht, hielt aber an weitgehenden Auflagen an Google Inc. (USA) sowie Google (Switzerland) GmbH im Rahmen der Aufnahmen für Street View fest.

Urteile des Bundesverwaltungsgerichts vom 30.3.2011 und des schweizerischen Bundesgerichts vom 31.5.2012

Die Gerichte bestätigten zunächst, dass das schweizerische Datenschutzgesetz (DSG) anwendbar ist, und dass auch gegen Google Inc., ein US-Unternehmen, in der Schweiz

geklagt werden konnte. Grundsätzlich stellen sämtliche nicht mit dem ausdrücklichen Einverständnis der betroffenen Personen im Internet publizierten Bilder aus dem Privatbereich einer Person eine Persönlichkeitsverletzung dar, gegen welche sich der Betroffene gerichtlich zur Wehr setzen kann.

Google wurde verpflichtet, im Bereich sensibler Einrichtungen wie Spitälern, Altersheimen, Schulen, Gefängnissen, Gerichten usw. sämtliche Bilder vor der Veröffentlichung im Internet vollständig – notfalls auch manuell - zu anonymisieren.

Bei Aufnahmen aus dem allgemeinen Öffentlichkeitsbereich erachtete das Bundesgericht die automatisierte Verwischung (Erfolgsfaktor ca. 99%) als genügende Massnahme. Es genüge, dass eine trotzdem erkennbare Person in einem einfachen, schnellen und kostenlosen Verfahren die nächträgliche Anonymisierung verlangen könne. Google wurde verpflichtet, ein solches Verfahren mit einem klar ersichtlichen Link einzurichten und regelmässig in grösseren Medien über die Möglichkeit zur Reklamation zu informieren.

Google wurde zudem verpflichtet, innerhalb von 3 Jahren alle Bilder aus dem nicht frei einsehbaren Privatbereich von Personen, insbesondere alle Aufnahmen von nicht allgemein einsehbaren Gärten, Höfen oder Innenräumen aus dem Internet zu entfernen.

Schliesslich wurde Google verpflichtet, vor künftigen Kamerafahrten die Bevölkerung der betroffenen Gebiete vorgängig durch die regionalen Medien zu informieren. Die Information auf der Internet-Seite von Google sei nicht ausreichend, weil niemandem zugemutet werden könne, sich im Internet vorgängig zu informieren.

Erkenntnisse

Das DSG ist immer dann anwendbar und auch ein Gerichtsstand in der Schweiz gegeben, wenn sich eine Massnahme in der Schweiz auswirkt. Eine betroffene Person ist auch

gegen einen US-Grosskonzern nicht schutzlos. Die schweizerischen Gerichte haben sich klar für den Persönlichkeitsschutz ausgesprochen, auch wenn ein öffentliches Interesse an Internet-Dienstleistungen wie Google „Street View“ anerkannt wird. Es ist jedoch eine Illusion, dass sich eine Einzelperson gegen Google, welche die besten Anwälte beschäftigen, wirksam zur Wehr setzen kann. Die Institution des Eidgenössischen Datenschutzbeauftragten, der kollektiv die Interessen vieler betroffener Personen wahrnehmen kann und zur Klage legitimiert ist, hat sich bewährt.

Summary in English

Since 2009 Google Inc. offers in Switzerland “street view”, which is a function of Google maps. With “street view” you virtually can walk through the streets and places in Switzerland. Faces of passer-by and vehicle numbers are smudged by the software automatically, but not with a 100%- success rate.

The Swiss Federal Data Protection Delegate sued Google Inc. in Switzerland because the Data Protection was insufficient in his view. The courts in Switzerland declared there competence. According to the applicable Swiss Data Protection Law Google Inc. and it’s Swiss subsidiary have been obliged by the courts, to fully make anonymous all faces and identification attributes in the environment of hospitals, homes for old people, schools, prisons and tribunals not only automatically by the software (with a 99%-success rate) but also with manual efforts, if necessary. For all other public areas Google has been obliged to install a simple and fast system – a clear link on the website – and without costs for reclamations for everybody who wants to be anonymous. Google has to inform about this option also in the classic medias (newspapers). Google has been obliged to

remove all pictures of not public (private) gardens, backyards and interior rooms within a period of three years from the internet. Google has finally been obliged to inform the inhabitants of the involved areas not only on the website but also in regional newspapers previous to all future tracking shots.

Dr. Paul Schaltegger
Zurich, Switzerland

Data Protection in Finland

Finland is believed one of the countries with the strictest data protection in Europe. Indeed, the Finnish legislation on data protection can be a nightmare for businesses, authorities and especially, for employers. Not only that there are several laws especially dealing with data protection and processing and privacy of communication but also that further provisions are found in other laws makes it difficult to find your way through the provisions, especially when you are a foreign business. Even where it becomes obvious that the protecting of data and privacy endangers businesses necessary amendments stuck halfway. Lex Nokia, for example.

Data protection is a legislative issue since 1988 when the Personal Data File Act was introduced to ensure for the first time in Finnish legislation the integrity of data processing and to establish data processing practices. The Finnish Constitution provides for an everyone´s fundamental right of privacy. According to the Constitution the secrecy of correspondence, telephony and other confidential communication is inviolable. Together with a reform of the Finnish Constitution the data protection in force by then was put in line with the EU Data Protection Directive´s (Directive 95/46/EC, and 1997, later amended in 2002) on June 1, 1999 when the act was replaced by the Personal Data Act. Also in 1999, the Law on Protection of Privacy and Data Security in Telecommunications was enacted. In 2001 the Act on the Protection of Privacy in Working Life was introduced, and renewed on October 1, 2004 which covers data protection issues and data processing procedures in the working life. Also in 2004 (September 1, 2004) an act on the Protection of Privacy in Electronic Communications came into force covering the confidentiality and privacy in telecommunications and establishing rules for processing confidential identification data and replaced the earlier act of 1999. On September 1, 2008, new legislation on how to process personal credit data was enacted. In addition, there are special provisions concerning the processing and storage of personal data in other laws and decrees as well. On the other side the Finnish legislation, i.e. the Act on the Openness of Government Activities, provides for a right to obtain information from authorities and access to public registers.

Especially the Act on the Protection of Privacy in Electronic Communicationscaused problems for data-sensitive businesses such as telephone operators, communication providers and technology companies. The privacy in electronic communications guaranteed confidentiality for both the content of the message and any identification data and covered all kind of “messages” (phone call, e-mail, SMS, or voice message or any comparable message transmitted between parties or to unspecified recipients in a communications network through which such message and data is not meant to be commonly available as well as so called “identification” data(data associated with an individual subscriber or user and which is handled in a communications networks for the purpose of providing the communication). The act allowed various exceptions but did not provide for clear guidance as to what was allowed under the exceptions and on how and under which circumstances to implement any of these exceptions. One of the main concerns was how to investigate suspicions of unauthorized disclosures of business secrets through by employees´ use of their e-mail accounts. This was a particular nightmare of technology companies, who are dependent on innovations and substantially invest in highly confidential research and development work.

The Finland based company Nokia was one of the main criticizers but denied that it was

pushing hard on public servants and ministers to achieve amendments. Together with other interest groupings this caused a broad discussion about the rights of the individual and the interests of business. As a consequence thereof a legislative committee was established very short after the act was introduced and drafted amendments to cover the problem of unauthorized data disclosures by employees by means of e-mails. The amendment essentially provides that a corporate subscriber has the right to monitor identification data automatically within the network if certain prerequisites are satisfied but a corporate subscriber is not allowed to read or open the content of the actual message.

The amendments the commission came up with allowed automatic monitoring provided that the employer (i) limits access to trade secrets and draft an adequate data security policy, (ii) identifies the persons having access to trade secretsand monitors only these people´s e-mails (iii) handles the issue in accordance with the provisions on internal co-operation withlabor representatives, (iv) notifies the office of the Finnish Data Protection Ombudsman and (v) gives a yearly report to the employees and to the data protection ombudsman of the actions under the amendment that have actually been undertaken. All of this was intended to give solely a right to manually review the identification data of specific messages but not the content. In addition, any breach or violation of the provisions were criminalized and subject to sanctions of up to three years imprisonment.

The amendments came into force on June 1, 2009 and were nicknamed Lex Nokia. Until today (end of 2013) there has been submitted one (1) notice to the Finnish Date Protection Ombudsman. This might be a result of the bureaucratic pre-requisits of such monitoring and on the limited possibilities of Finnish police to start investigations. The police may not investigate telecommunication or identification data in case of company espionage as the maximum sanction for company espionage is two (2) years; telecommunication date surveillance and investigation requires the possibility of a criminal offence with a sanction of at least four (4) years. This will change in 2014 to two (2) years.

For Finnish and foreign employer the privacy and confidentiality of e-mail and similar electronic communications is until today a problem. The e-mails of the employee may not be reviewed by the employer and in the case of sickness leave, holiday or even after termination the employee´s e-mails may not be opened in the case it can be deemed private on the basis of its identification data. Even in the case an e-mail can be clearly identified as business e-mails special procedure ought to be obtained in order to allow the employer to respond or read the content thereof. In consequence, employee´s should not be given any "own" (firstname.surname @employer) address as it is privacy protected. In addition, the use of the employers e-mail address shall be prohibited for private purposes. As this is not always practicable, employers should take precaution when organizing and establishing communication means for their employees.

Gerrit van Setten
Helsinki, Finland

Réedition

LA PROTECTION DES DONNEES PERSONNELLES DANS L'ENTREPRISE

C'est trois ans après le rapport Nora-Minc

1978 sur l'informatisation de la société, que se situe l'intitiative du Conseil de l'Europe ayant promulgué une Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. A la suite de cette exigence l'Union Européenne a promulgué la directive 95/46/EC.
Sous la responsabilité du CNIL (Commission Nationale Informatique et Liberté) la question de la protection des données personnelles et de la vie privée **au travail** a fait l'objet d'une reflexion approfondie a l'occasion d'une réunion le 28 janvier 2013.
Cinq problématiques ont alors été traitées par la CNIL :

A) Le recrutement et la gestion du personnel (The hiring procedure and managing of employee)

Dans ce contexte la CNIL impose que les données soit uniquement destinées à évaluer la capacité du candidat à occuper l'emploi proposé. Ainsi est-il interdit d'interroger un candidat à un travail quant à son numéro de sécurité sociale, ses opinions politiques ou son l'appartenance syndicale.
Quant à l'accès aux données ? Il s'agit d'un accès limité aux seules personnes intervenant dans le recrutement. Ce sont les personnes chargées de la gestion du personnel lesquelles peuvent consulter ces informations dans l'exercice de leurs fonctions. Elles ont accès aux données figurant dans le registre unique du personnel comme par exemple le nom, la nationalité, la fonction occupée, la date d'entrée dans l'organisme. Les autres instances peuvent obtenir certaines informations pour exercice de leur fonction.
L'employeur doit assurer la sécurité des informations et garantir que seules les personnes habilitées puissent en prendre connaissance. Chaque consultation doit être enregistrée et les données sont automatiquement détruites deux ans après le dernier contact. Les informations sur un employé ne sont conservées que le temps de sa présence dans l'organisme.
Néanmoins une fois l'employé parti certaines informations doivent être conservées plus longtemps par l'employeur. Par exemple les bulletins de paie doivent être conservés pendant 5 ans après le départ du salarié.

B) La géolocalisation des véhicules (The localization of vehicle by mean of satellite).

De nombreuses règles encadrent l'utilisation de ces outils afin que la vie privée des employés soit respectée et l'installation d'un appareil de localisation dans un véhicule est subordonnée à des justifications.
Ainsi l'installation est permise pour :

- Suivre et facturer une prestation de transport de personnes
- Assurer la sécurité de l'employé, des marchandises ou des véhicules dont il a charge
- Mieux allouer des moyens pour des prestations à accomplir en des lieux dispersés
- Suivre le temps de travail
- Respecter une obligation légale ou réglementaire

Mais ne peut pas être utilisée pour :

- Pour contrôler le respect des limitations de vitesse
- Pour contrôler un employé en permanence
- Pour calculer le temps de travail

Afin de garantir ses droits les employés peuvent s'opposer à l'installation d'un tel dispositif dans leur véhicule dans le cas où ce dispositif ne respecte pas les conditions légales posées par la CNIL ou d'autres textes.
L'accès aux informations du dispositif de géolocalisation doit être limité aux services concernés et à l'employeur. En outre il est impératif de prendre des mesures de sécurité.
En principe, la durée de conservation ne doit pas dépasser plus de deux mois. Toutefois, ils peuvent être conservés au maximum cinq ans s'ils sont utilisés pour le suivi du temps de travail.

C) Les outils informatiques au travail (computer in the working environment).

En ce qui concerne l'utilisation personnelle de ces outils c'est à l'employeur de fixer les limites de cette tolérance et d'en informer des employés.
L'employeur peut contrôler et limiter l'utilisation d'internet et de la messagerie pour assurer la sécurité des réseaux qui pourraient subir des attaques et pour limiter les risques d'abus d'une utilisation trop personnelle d'internet ou de la messagerie.
Par défaut, les courriels ont un caractère professionnel. L'employeur peut les lire, tout comme il peut prendre connaissance des sites consultés, y compris en dehors de la présence de l'employé.

Quand même il y a des limites au contrôle de l'employeur. L'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses employés, cela serait excessif. En outre, les logs de connexion ne doivent pas être conservés plus de 6 mois.
Notamment l'employé a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées. Par conséquent, un employeur ne peut pas librement consulter les courriels personnels de ses employés, même s'il a interdit d'utiliser les outils de l'entreprise à des fins personnelles. Cela ne s'applique qu'à condition d'en avoir ajouté la notion « Personnel » ou « Privé ».
Quant aux fichiers ils ont, par défaut, un caractère professionnel et l'employeur peut y accéder librement.
Les identifiants et mots de passe sont confidentiels et ne doivent pas être transmis à l'employeur, sauf si l'employé détient sur son poste des informations indispensables à la poursuite de l'activité.

D) L'accès aux locaux et le contrôle des horaires (access to working area and the control of working time).

Les contrôles d'accès et du temps de travail existent depuis bien longtemps et les technologies qui facilitent ces contrôles permettent la collecte de toujours plus d'informations.
L'employeur peut mettre en place des outils – y compris biométriques – de contrôle individuel de l'accès pour sécuriser l'entrée dans les bâtiments et les locaux faisant l'objet d'une restriction de circulation.
Toutefois le système ne doit pas servir au contrôle des déplacements à l'intérieur des locaux.
L'accès aux informations n'est ouvert qu'aux membres habilités des services gérant le personnel, la paie ou la sécurité. L'employeur doit prévoir des mesures pour assurer la sécurité des informations concernant ses salariés.
Les données relatives aux accès doivent être supprimées 3 mois après leur enregistrement. Par contre les données utilisées pour le suivi du temps de travail doivent être conservées pendant 5 ans.

E) La vidéosurveillance – (The video control camera in the working area).

Les environnements de travail sont de plus en plus équipés de dispositifs de vidéosurveillance. Bien que légitimes pour assurer la sécurité des biens et des personnes, de tels outils ne peuvent pas conduire à placer les employés sous surveillance constante et permanente.
Les caméras peuvent être installées au niveau des entrées et sorties des bâtiments, des issues de secours et des voies de circulation ainsi que des zones où de la marchandise ou des biens de valeur sont entreposés.
Surtout elles ne doivent pas filmer les employés sur leur poste de travail, sauf circonstances particulières (par exemple employé manipulant de l'argent). Les caméras ne doivent pas non plus filmer les zones de pause ou de repos des employés, ni les toilettes.
Seules les personnes habilités et dans le cadre de leurs fonctions peuvent visionner les images enregistrée.
La conservation des images ne doit pas excéder un mois. En règle générale, conserver les images quelques jours suffit à effectuer les vérifications nécessaires en cas d'incident, et permet d'enclencher d'éventuelles procédures disciplinaires ou pénales.

On the 28 january 2013 the CNIL (Commission National Informatique et Liberté) organized a european conference (7èm journée européenne de la protection des données personnelles et de la vie privée) enphasizing the need for data

protection in the working environment. The CNIL had noted in 2012 that more than 10% of all contests brought to her were connected to the working environment and 17 had led to some injunction to the managers. (for some false information or lack of information, non appropriate, or excessive collect of data) Following this conference CNIL published five leaflets with guidance and restriction rules related

to data collection and use in

- **The hiring procedure and managing of employee**
- **The localization of vehicle by mean of satellite.**
- **Computer tools in the working environment.**
- **The access to working premises and the control of working time.**
- **The video control camera in the working area**.

Leonard Goodenough
Paris, France

Published by:
ULN united.legal.network.EEIG
Hohenstaufenring 63, 50674 Köln / Cologne - Reg. Cologne HR A 14903
Austria, Belgium, Bulgaria, Czech Republic, Finland, France, Germany, Greece, Hungary, Italy, Luxembourg, Netherlands, Norway, Poland, Romania, Slovenia, Spain, Switzerland, United Kingdom, Turkey

Authors:

Andrea Hellmann, Rechtsanwältin, Martiusstraße 5, 80802 Munich, Germany
E-mail: ahellmann@law-wt.de

Dr. Paul Schaltegger, Rechtsanwalt, Florastrasse 49, 8008 Zurich, Switzerland
E-mail: paul.schaltegger@sbrs.ch

Gerrit van Setten, Attorney-at-law, Kansakoulukuja 3, 00100 Helsinki, Finland
E-mail:gerrit.vansetten@vsp-law.com

Leonard Goodenough, Avocat à la Cour, 5 rue Taylor, 75010 Paris, France
E-mail: leonard.goodenough@avocat-taylor.com