European Data Protection Update

Contents Page

INTRODUCTION

In this age of big data and data analytics, organisations recognise the value of data and more importantly, personal data, whether those organisations are in the public or private sector. However, for organisations with a pan-European presence, keeping up-to-date with each country's data protection legislation and best practice can seem like an impossible task.

For some time Europe has been discussing proposals to reform data protection law and it was as long ago as January 2012 that proposals for European data protection reform were launched. The main proposal involved a General Data Protection Regulation (the GDPR). It was the intention that the use of a Regulation rather than a Directive would give consistency to data protection laws throughout the EU that many feel is currently lacking and is the cause of much confusion and uncertainty.

More than three years after the launch, discussion on the new GDPR continues at the European Council level and it is likely to be many months yet before the final GDPR is brought into law.

As a result, the data protection regimes operated by countries throughout the EU and indeed, throughout the EEA, vary considerably both in terms of the detail of their respective legal frameworks and in terms of enforcement for breaches of the relevant framework.

We have collaborated with a number of leading law firms across Europe to create this European Data Protection Update publication. In this publication we highlight a number of key developments which have happened recently or which are about to happen, as well as providing a summary of some interesting cases that may impact on the relevant data protection regimes in the coming months.

Contact details for all of the contributor firms are provided within this publication, so please do get in touch if you have any questions or require any advice.

In the meantime, we wish you all the best.

> The most valuable commodity I know of is information
>
> Gordon Gekko, Wall Street (1987)

This brochure contains a summary of general principles of law. It is not a substitute for specific legal advice, which should be sought in relation to any application of the subject matter of this brochure.

AUSTRIA

DORDA BRUGGER JORDIS

Axel Anderl
Partner
T +431 533 479 523
E axel.anderl@dbj.at

On the horizon

Standard Applications for banking processing?

As a general principle all data processing in Austria has to be notified to the Data Protection Authority (the DSB). In order to minimize the amount of required notifications for common, day to day processing, Austrian data protection law provides for a so called Standard and Model Application Decree. This contains 36 standard types of data processing that do not have to be notified, as long as processing of personal data is within the identified scope. Unfortunately none of these standard exceptions covers the day-to-day business of banks. To be fully compliant, a bank doing business in Austria actually requires between ten and twenty notifications. The DSB is currently considering the establishment of specific standard exceptions for the banking and regulatory sector. This would potentially relieve Austrian banks of the need to notify their usual core activities as these would be covered by the new exceptions. However, the standard types of data processing exceptions usually limit the number of recipients of data which can be covered by the exception. Thus, international banks might still fall outside the benefit of such exceptions because of the scale of transfers of personal data within the group.

From official secrecy to freedom of information?

The Austrian Government is currently discussing a change to the constitutional principle of official secrecy – no right to information held by administrative bodies – to limited freedom of information. Specific administrative bodies shall be obliged to publish information of public interest, as long as no specific duty to maintain confidentiality is established by law. Information may only be withheld from disclosure as a result of (i) overriding legitimate interests in maintaining the secrecy of personal data of data subjects, (ii) external political reasons, (iii) reasons of national security or (iv) the existence of business and/or trade secrets. In addition, publication may be denied if the effectiveness of investigations may be compromised. Other factors to be considered are ensuring that the decision making process is unaffected, maintaining the stability of the financial market and ensuring fair competition. As many administrative authorities, including the DSB, have filed concerns and requests for clarification of the proposal it is not expected that the new laws will enter into force before late 2015.

Cases

Stringent rules on CCTV

The DSB is, in general, very concerned about the installation of CCTV, especially where public areas are to be monitored. In a recent case regarding "Dashcams" it was held that no private data controller is allowed to monitor any public area, even where it does not happen intentionally and the data is encrypted. The use of CCTV in public areas is reserved to the national security agencies, only. As a result, any provision of (e.g. insurance) services that may require the installation of CCTV within cars or other vehicles cannot be imposed in Austria.

In addition, the DSB has frequently held that in the case of monitoring of shop windows and entrances to offices, shops or other buildings, no more than 50cm of public area may be captured. Even if just a small public area is under surveillance for a legitimate purpose the DSB might nonetheless refuse the mandatory registration of such a CCTV system.

Approval for data processor

Every data transfer – irrespective of whether controller-to-controller (C2C) or controller-to-processor (C2P) – to a recipient based outside the EEA in a country without an adequate level of data protection requires the prior approval of the DSB. In general, a data controller is obliged to request such approval for the transfer of personal data for a specified purpose. Although Section 13 paragraph 4 of the Austrian Data Protection Act provides data processors the right to apply directly for such an approval, where they carry out similar data processing activities for multiple data controllers, the formal requirements for such requests have as yet not been fully developed.

The DSB rendered a decision on 5 September 2014 granting a data processor approval to transfer data of a specific data controller to a sub-processor situated outside the EEA. It is anticipated that many similar decisions will follow, as it is of crucial importance/value for data processors situated outside the EEA to have pre-existing approvals for potential sub-processors in place, instead of having to force each customer (data controller) into cumbersome and lengthy approval proceedings in each and every single case.

BELGIUM

ALTIUS
ADVOCATEN | AVOCATS | LAWYERS

Gerrit Vandendriessche
Senior Partner
T +322 426 1414
E gerrit.vandendriessche@altius.com

On the horizon

Privacy part of coalition agreement

When it came into power in October 2014, the new Belgian government underlined the importance of privacy in its government program. It underlined privacy as a fundamental right in the digital economy and especially in light of the (ab) use of big data, both in the public and the private sector. The government advocated a harmonization of privacy laws throughout the EU, although each EU member state should still be able to go beyond the EU framework when it concerns social security, health and government purposes.

According to the new government, informed consent should be the primary basis for any processing. Apart from references to some existing privacy rights, the new government also intends to work on some new rights, such as the right of the data subject to contextuality and portability of their personal data. Finally, the government also announced its intention to reform the Belgian data protection authority.

Cookies

Contrary to most EU countries, there was no guidance from the regulator in Belgium on how cookie consent and information should be handled. The Belgian data protection authority recently published a draft advice on the legal aspects of cookies. The draft was published for consultation and is expected to be put in a final version soon.

Cases

Right to be forgotten

Long before the ECJ Costeja decision, Belgian courts had rendered judgments regarding the right to be forgotten principle.

Recently, a Belgian court of appeal ordered a newspaper to anonymize the name of a physician in an on-line press article (not to withdraw the article). The article reported that the physician caused a car accident as a result of being drunk whilst driving, which resulted in a number of fatalities. The accident and the press article dated from 1994 but in 2010 the physician requested the newspaper to anonymize it, a request that was refused by the newspaper. The court considered that the newspaper was liable on a non-contractual (tortious) basis for having refused the anonymization as a result of a number of factors: (a) sufficient time had elapsed between the accident and the request for anonymization being made; (b) the doctor's lack of public personality; and (c) the lack of added value of the information for the public.

Contrary to the ECJ Costeja case, the Belgian court recognized that newspapers are also subject to the principles of the right to be forgotten. The newspaper tried to shift the responsibility for the article being accessible online to the web search engines, but the court considered that since the newspaper was at the basis of the publication, it was ultimately responsible.

CZECH REPUBLIC

KOCIÁN ŠOLC BALAŠTÍK
ADVOKÁTNÍ KANCELÁŘ

Drahomir Tomasuk
Counsel
T +420 224 103 316
E dtomasuk@ksb.cz

On the horizon

Open accounts vs. Personal Data Protection

Open accounts have become the norm for certain entities in the Czech Republic (typically political candidates running for election) as such accounts can be scrutinised on a voluntary or statutory basis. This allows the finances of parties and individuals alike to be subject to public scrutiny. According to the Czech Data Protection Authority (the CDPA), such transparency measures may conflict with personal data protection requirements regarding data about the other party to a financial transaction. If the payment data unambiguously identifies the sender/recipient, it is deemed to constitute personal data (as per the Czech Personal Data Protection Act). The CDPA has therefore ruled that the entity about whom the accounts are being prepared must obtain consent from the sender/recipient before such data can be included in the open accounts.

Requests for consent to personal data processing often made unnecessarily

Many data controllers requests for consent are unnecessary, resulting in a breach of applicable law. Controllers are generally required to process personal data based on legal grounds, with consent being one such ground (others are listed by special law). However, data controllers often have trouble correctly identifying whether special legal grounds exist for processing the data without the data subject's consent, and consequently request consent from the data subject unnecessarily. One of a data controller's duties is to inform the data subject of the data controller's obligation to disclose the personal data in cases where the special law so requires and if the data controllers seek consent then they often fail to do this. Hence, not only are a data controller's actions unnecessary, they are often even misleading (and in conflict with the law). The CDPA has indicated that where such conduct is identified the data controller may be ordered to rectify the position and that penalties may be imposed to ensure compliance with the relevant statutory duties.

Cases

Is information stored in the cloud by a lawyer safe?

When providing legal services Czech lawyers are increasingly using cloud services. However, the future of this trend has been put in jeopardy due to one very controversial decision by the Municipal Court in Prague. Can cloud storage on a third-party server be considered to be a place where the lawyer carries out his/her profession and which, as a result, enjoys special protection in criminal proceedings? The Criminal Procedure Code requires that a search of such premises must be attended by a representative of the Czech Bar Association, and the representative also has the power to grant consent to or refuse any review of confidential documents. Nevertheless, the Court held that the cloud is not such a place and hence is not subject to any special protection during police investigations.

Unlawful disclosure of information that a certain individual is HIV positive

The Czech Supreme Administrative Court (the SAC) recently dealt with a conflict between information allegedly disclosed in the interests of public health and the protection of personal data. The case concerned a sixteen-year old boy who the police first reported had gone missing and that he suffered from a serious contagious disease (no details were disclosed). Based on the information disclosed by police, a Czech TV station ran a story in which it disclosed the boy's full name and stated that he was HIV positive. The SAC, in upholding the fine imposed upon the TV station by the CDPA, held that rather than generally describing the health hazards resulting from contact with the missing person, the TV station endeavoured to excite and frighten the viewing public as much as possible in order to increase its ratings. The SAC held that the story was not in proportion to the public's legitimate interest in the protection of public health and harmed the missing boy's right to the protection of sensitive personal data.

DENMARK

PLESNER

Michael Hopp
Partner
T +453 694 1306
E mho@plesner.com

On the horizon

DPA focus on data breaches

The Danish Data Protection Agency (the DPA) has announced that it has noted an increase in the last year in the number of data breaches. As a result the DPA has indicated that making sure that data controllers take the appropriate steps when faced with a data breach will continue to be part of its enforcement focus. The DPA recommends that a data controller faced with a data breach assesses which specific initiatives may be appropriate in order to alleviate the detriment to any affected data subjects and takes the necessary steps to ensure that future data breaches are avoided.

Parliamentary Working party on Data Security

Recently a cross-party Parliamentary Working Group on Data Security issued a report listing its findings on the level of data security compliance in the public and private sectors. The report was generally very critical of both sectors' level of compliance with data protection law, in particular the lack of protection against outside threats (hackers) and the public sector's oversight of its private sector service providers. The report issued a number of recommendations which included increasing the funding of the DPA, introducing criminal penalties for public sector data controllers and their processors, removing the DPA from under the oversight of the Ministry of Justice and placing it under the Parliament and grouping the ministerial responsibilities for data security under one Ministry. The recommendations are unlikely to become a reality this side of the upcoming Parliamentary election which will take place before the end of 2015.

Cases

Hacking of key government databases

The DPA is currently investigating what has been claimed to be the largest hacking incident in Danish history which came to light more than a year ago. The incident involved the compromising of several large public sector databases including the Schengen register and the database of issued drivers licences. The matter has already led to the criminal conviction of the main suspect, following his extradition from Sweden. However, the DPA's investigation is dragging on, presumably in light of the complexity of the matter and the limited enforcement tools available to the DPA as regards data processors acting on behalf of public sector data controllers, (as noted this is one of the difficulties highlighted by the Parliamentary Working Party on Data Security).

New guidelines

The DPA has recently instituted new guidelines regarding the processing of employee related data. The guidelines elaborate and specify the data security requirements for such data required by Danish data protection law. Amongst other things the guidelines require that the data controller describes how the data security requirements are complied with, reflecting the accountability approach to data protection which the EU General Data Protection Regulation is expected to contain.

ESTONIA

Pirkko-Liis Harkmaa
Associate Partner
T +372 630 6460
E pirkko-liis.harkmaa@lawin.ee

On the horizon

Implementation of cookie requirements

Estonia has still not enacted any explicit legal provisions concerning the use of cookies on websites as provided for in the ePrivacy Directive (2002/58/EC). A draft bill covering these issues was under discussion during 2014 however the proposed amendment to the Estonian Information Society Services Act which would have implemented Art 5(3) of the ePrivacy Directive has been discarded. Thus, at this time it is still uncertain whether and when legislation concerning the use of cookies will be enacted in Estonia. Until then, the use of cookies continues to fall outside any specific regulation in Estonia.

Supervisory activities of the Estonian Data Protection Inspectorate

In a news item on its webpage, the Estonian Data Protection Inspectorate (the DPI) has given an indication of the principles it will apply when dealing with complaints which allege defamation, for example in blog posts. In line with the new Law Enforcement Act that entered into force in 2014, the violation of a specific individual's subjective rights should be taken up by a regulatory authority where: (1) judicial legal protection is not possible in a timely manner, (2) if the regulatory authority does not take action exercise of a right is impossible or significantly complicated, and (3) it is in the public interest to take the action on behalf of the individual. According to the DPI, in the case of defamatory blog posts, however, the criterion of public interest is seldom fulfilled; therefore, in such cases the DPI would not take regulatory action and the injured party should instead take their own action through the civil courts.

Cases

Re-using publicly available data

In a recent case, the Supreme Court clarified the rules of processing personal data which has been made publicly available.

The case was raised by a convicted offender imprisoned for life, as a result of a documentary aired on public television which depicted his crimes. The offender claimed inter alia that his name and image was unlawfully used. The TV channel which aired the documentary disagreed on the grounds that the information was obtained from a publicly available court decision and the purpose of the documentary was to prevent serious crimes by informing the public.

Indeed, the Personal Data Protection Act (the PDPA) provides that personal data may be processed and disclosed in the media for journalistic purposes without the consent of the data subject if: (a) there is predominant public interest; (b) it is in accordance with the principles of press ethics; and (c) the disclosure of the data does not cause excessive damage to the rights of the data subject. Furthermore, as a rule, if certain personal data is made publicly available, the provisions of the PDPA do not apply in respect of processing of such data.

However, the Supreme Court explained that even if the personal data of an individual has been made public lawfully but without the data subject's consent (e.g. in the course of a public hearing in criminal court proceedings), this does not mean that such personal data could be further publicised repeatedly and without any limitations. According to the Court, such an absolute right would be in conflict with the general principles of data protection law. The Court noted that the further disclosure of personal data publicised in a court hearing e.g. in printed media or television would significantly broaden the circle of individuals that are made aware of the information and thus it could have severe consequences for the data subject.

FINLAND

JP Alho
Partner
T +3582 9000 6264
E jp.alho@krogerus.com

On the horizon

Remainder of the Information Society Code to enter into force

The Information Society Code was enacted into law in November 2014. The Code is a complete reform of legislation applying to electronic communications. It repeals eight previous acts, including the Act on the Protection of Privacy in Electronic Communications which transposed the ePrivacy Directive 2002/58/EC into national law, and integrates their provisions into one Act. The Code takes the same approach taken in the proposed General Data Protection Regulation, so that the majority of the ePrivacy sections of the Code apply also to operators not established in the EU but whose users are in, and whose service is targeted at, Finland. The main part of the Code entered into force at the start of 2015, but the new provisions concerning communications service agreements take effect from July.

Government proposal on revision of appeal rules in data protection matters

Finland has in place a two-tier system of data protection authorities: the Data Protection Ombudsman (the DPO) provides direction and guidance on and supervises the processing of personal data, whereas the Data Protection Board (the DPB) deals with questions of principle and makes final decisions. Under present law certain decisions of the DPO and the DPB are subject to appeal to an administrative court, and appeal against a decision of an administrative court may be lodged in the Supreme Administrative Court. The Government has put forward a bill to revise the appeal rules in administrative matters which, if passed by the Parliament, would have significant implications for data protection laws. Under the proposal, all decisions of the data protection authorities, including those related to their rights of access and inspection, would be subject to appeal, but in order to appeal against a decision of the administrative court, leave of appeal would need to be requested from the Supreme Administrative Court. The proposal is currently in committee debate.

Cases

Sensitive data

The Finnish Supreme Court very rarely has to deal with data protection matters, previous cases date back to 2004 (dealing with processing of personal identity numbers) and 1999 (addressing a personal data offence). In November 2014, however, the court gave its ruling in criminal proceedings against a physician who had read the patient information of a person who was being treated at his clinic but who was not his patient. Lower courts had held that the prohibition on processing sensitive data only permits a health care professional to process patient documents if that is necessary for the treatment of the patient. The Supreme Court disagreed, holding that the requirement of necessity related to data content, not the individual acts of processing. The principle of purpose specification laid down in the Personal Data Act (the PDA) must, however, be taken into account.

Controller in direct marketing

Where personal data is obtained from a third-party database for direct marketing purposes, who is to be considered as the controller? The PDA defines controller as a person for the use of whom a personal data file is set up and who is entitled to determine the use of the file. In the ACC Consulting case the DPB decided that what matters is who determines the purposes and means of the processing operation on a case-by-case basis and therefore the marketer is a controller. As a controller, the marketer is under an obligation to see that the data subjects can exercise their right to object to the processing of their personal data for direct marketing purposes laid down in the PDA.

FRANCE

JEANTET ASSOCIÉS

Isabelle Pontal
Counsel
T +33 01 45 05 81 05
E ipontal@jeantet.fr

On the horizon

Legal framework for geolocation operations

Bringing together recent judgements of the European Court of Human Rights and the French Supreme Court (Cour de Cassation), a new law (Law No. 2014-372 of 28 March 2014) was enacted to provide a legal framework for geolocation operations performed in real time. These laws will apply to operations which are intended to follow at any time the movements of an object and, where applicable, the person who owns it.

Various real time geolocation techniques can be implemented during criminal investigations, including, for example, the use of a geolocation dedicated device (a marker) placed on a means of transportation or any other object.

The law adds new Articles to the French Code of criminal procedure (the CCP) (Articles 230-32 to 230-44) which provide that geolocation measures can be ordered by the court as part of a non-covert or preliminary investigation, and as part of a judicial investigation.

Furthermore, as with telephone interceptions, geolocation measures are not only available to be used in respect of people suspected of having committed an offence, but can also be used in connection with any individual (in particular family or friends of the suspect) as soon as the needs of the investigation so require.

Cases

Proper use of CCTV systems

In December 2013, the Company APPLE RETAIL FRANCE was the subject of the first formal notice from the French data protection authority (the CNIL) in connection with the video surveillance system installed to monitor employees in the APPLE STORE, in Opéra, Paris. The CNIL ordered in particular that Apple redirect some of the cameras that constantly filmed employees and also that they must inform the employees of the existence of the video surveillance devices.

In February 2014, Apple advised that it had complied with its obligations concerning the store targeted by the formal notice, leading to the closure of the formal notice. However, inspections conducted in May and June 2014 in other APPLE STORE stores have revealed that the company had not adopted similar compliance measures in all its stores. The persistence of these failures led the CNIL, on 14 October 2014, to issue another formal notice to the company requiring that it revise the entire video surveillance systems of its 16 stores in France.

The CNIL was asked by the Rhône-Alpes labour inspection board to review the video surveillance systems used in the subsidiaries of the company Providis Logistique. The inspections conducted by the CNIL at the premises of the company and certain of its subsidiaries revealed numerous breaches of the French Law on IT and Freedoms. The CNIL therefore issued a formal notice to Providis Logistique on 12 July 2013.

In responding to this notice, the company reported that it had corrected some failures. However, more recent inspections of the premises revealed the persistence of certain failures; in particular, the company kept on continuously filming certain areas reserved to employees (access to locker rooms and spaces dedicated to the rest of employees). The CNIL considered that no particular justification could validate such an invasion of privacy of the employees concerned. It also considered that the information on these systems was incomplete and security measures to ensure the confidentiality of the data generated by the systems used were insufficient. Therefore, the CNIL imposed a fine of EUR 5,000 against Providis Logistique.

GERMANY

HEUKING KÜHN LÜER WOJTEK
LAWYERS AND TAX ADVISORS

Astrid Luedtke
Lawyer
T +49211 600 55 168
E a.luedtke@heuking.de

On the horizon

Draft Bill for IT Security Act

The Federal Ministry of the Interior presented a draft bill of an IT Security Act on 18 August 2014. The IT Security Act aims to protect critical infrastructures which are considered to be the backbone of digital society. Providers of critical infrastructures will need to meet certain standards of IT Security and notify the Federal Office for Information Security (the BSI) of IT security related incidents. The BSI will collect that information and share the experience amongst the providers of other critical infrastructures to allow them to enhance their protection.

Draft Bill confirms Data Protection law to be Consumer Protection law

In February 2015, the Federal Cabinet agreed a draft Bill aimed at improving enforcement of data protection laws protecting consumer interests. Under the draft Bill all data protection rules and regulations that apply to processing of personal data by a company for commercial purposes such as advertising, marketing, market or opinion research or the creation of user profiles, are considered consumer protection provisions. As a result, injunctions based on protection of consumers' interests may be sought by competition associations or other registered qualified bodies within the meaning of Art 4 of the Injunctions Directive (98/27/EC).

Cases

Is an IP-Address personal data?

In Germany there has been considerable discussion over whether a dynamic IP address is "personal data". The Federal Court of Justice has now referred this question to the European Court of Justice. The Federal Court of Justice had to decide whether the Federal Republic of Germany may save the IP addresses of visitors to governement websites beyond the termination of the respective user's activity. The first question referred is whether, according to Art. 2a of the Data Protection Directive (95/46/EC) an IP address which a service provider stores in connection with a visit to its website is deemed personal data held by the service provider if it is not the service provider but only a third party who has the additional knowledge necessary to identify the person concerned. The second question referred relates to Section 15, para 1 of the German Telemedia Services Act, and the question of whether Art. 7f of the Data Protection Directive permits personal data of a user of telemedia services to be stored without their consent (other than for the data subject's actual use of the service) for the general purpose of maintaining the security and functionality of the telemedia service.

Use of Facebook fan pages does not lead to data protection responsibility

In September 2014 the Higher Administrative Court of Schleswig confirmed that a company that operates a Facebook fan page is not responsible for how the personal data of visitors to the page is processed, because it has no influence on the data processing by Facebook. The fact that the operator of the fan page receives anonymized statistics about Facebook users does not create a data protection responsibility. The Court went on to say that the Data Protection Commissioner for the German state of Schleswig-Holstein (ULD) which had started ordering companies in 2011 to deactivate their Facebook fan pages is not allowed to do that.

Permanent video surveillance through a dash cam unlawful

Permanent surveillance of traffic through a dash-cam in a car is unlawful, the Administrative Court of Arnsbach and the District Court of Munich ruled in two recent decisions. Both courts ruled that permanent recording of the public sphere by dash cams in cars, which necessarily covers innocent bystanders, is not justified by the interest of the dash-cam user in securing evidence.

HUNGARY

SZECSKAY ATTORNEYS AT LAW
WWW.SZECSKAY.COM

Dr. László Pók
Partner
T +361 472 3000
E laszlo.pok@szecskay.com

On the horizon

Fee to be introduced in respect of the data protection register of the DPA

Under the Hungarian Privacy Act, data management and processing activities, with some exceptions defined in the Privacy Act, must be registered in the data protection register kept by the Hungarian National Authority for Data Protection and Freedom of Information (the HDPA). Currently, there is no fee payable in respect of the notification made to the data protection register, although the Privacy Act allows for the introduction of such fee by a ministerial decree (which has not yet been adopted). Therefore it is expected that once such a ministerial decree is adopted, the notification to the data protection register will be subject to a fee.

Data protection issues concerning the use of drones

In November 2014 the HDPA issued guidance on data processing by the use of drones. This guidance covers the use of drones for general purposes and also for commercial purposes. It also provides proposals for legislation to regulate the use of drones from a data protection perspective. According to the HDPA, in connection with the processing of the data collected by the use of drones, the time frame, location and people who may be affected, should all be clearly defined. To ensure lawful data processing, the HDPA proposes a licensing procedure for the use of drones by the aviation authority. It is also recommended by the HDPA that an identification system for the drones should be introduced.

Cases

Heavy fines in the procedures of the Hungarian DPA

Since 1 January 2012 the HDPA has been entitled to impose fines relating to unlawful data management up to an amount of HUF 10,000,000 (approx. EUR 33,000). Since that date, the HDPA has imposed high fines in several cases. This is particularly true for 2014, when many cases resulted in the imposition of significant fines, particularly in respect of data management by companies which organise product introductions and companies providing debt collection services. In most cases the problem lay in the lack of a legal basis for the data processing (i.e. there was no consent to and no information provided on the details of the data processing). The fine was close to the upper limit in cases where the illegal data processing investigated by the HDPA concerned a large number of data subjects, sensitive personal data and where the infringement was multiple (i.e. where multiple provisions of the Privacy Act were infringed) and/or of a repeated nature. For example the maximum fine was imposed in a case where a large number of data subjects provided their personal data to the data controller who then, without appropriate consents, transmitted such personal data to a number of further data controllers for direct marketing purposes.

Whistleblowing

The legislation which created a statutory legal basis for the establishment of whistleblowing systems by employers (so that no consent from employees is required if the conditions listed in the relevant act are met) came into force in January 2014. In its recent opinion, the HDPA made it clear that information on the whistleblowing system (e.g. procedural rules) must be published on the website of the organisation using the whistleblowing system. This means that publication on an internal system (e.g. intranet) is not sufficient. It is also noted by the HDPA that data can only be transferred abroad if the foreign data controller or data processor operating the whistleblowing system for the employer undertakes to comply with both the provisions of the whistleblowing legislation and the provisions of the Privacy Act.

IRELAND

A&L Goodbody

Mark Rasdale
Partner
T +353 1649 2300
M+3161 138 8597
E mrasdale@algoodbody.com

On the horizon

Increased government focus on data protection

2014 saw the appointment of Ireland's first female Data Protection Commissioner, Helen Dixon. The 2015 Irish Government Budget has doubled the funding for the Data Protection Commissioner (the ODPC). Regulator profile, investigations and enforcement actions are likely to increase.

Data protection audits

In August 2014, the ODPC published an updated version of their 2009 Guide to the Audit Process to reflect developments in the legislation and changes in the approach of the ODPC to the audit process.

2013 saw a 10% rise from 2012 in the number of audits carried out by the ODPC to 44. The legal basis for the audits is contained in Section 10 (1A) of the Irish Data Protection Acts 1988 and 2003 (the DP Acts). It is anticipated that the level of audit activity in Ireland will continue to increase.

Cyber crime and cyber security

Ireland is required to transpose Directive 2013/40/EU on Attacks against Information Systems by 4 September 2015. The Directive has introduced new crimes such as botnet attacks and identity theft. An obligation has also been imposed on Member States to respond to urgent information requests within eight hours and to collect basic statistical data on national cybercrime.

Cases

First data protection convictions against company directors

In October 2014, the ODPC secured its first personal convictions against company directors for their part in the breach of data protection law by their private investigation company. The company was charged with 23 counts of breaches of section 22 of the DP Acts for obtaining access to personal data without the prior authority of the data controller and disclosing the data to another person. Separate prosecutions were made under section 29 of the DP Acts, which provides for prosecution where the corporate offence is committed with the consent or connivance of, or is attributable to any neglect on the part of the directors or other officers.

Irish Government involvement in the Microsoft warrant case

The Irish Government has filed an amicus curiae brief in relation to the US Court of Appeal case Microsoft v the United States. The amicus curiae concept allows a party to offer a position on a case that it is not directly involved in, which in this case is the ongoing legal dispute between the US and Microsoft over access to an email account held on an Irish server.

Ireland refers safe harbour question to the court of justice

In the case of Schrems v the Data Protection Commissioner, the Irish High Court had to consider whether the ODPC was correct not to investigate and stop the transfer of personal data from Facebook Ireland to its parent company in the US. The basis for the challenge to the transfer was that there is no effective data protection regime in the US.

In his decision on 18 June 2014, Mr Justice Hogan concluded that if the ODPC cannot arrive at a decision that is inconsistent with a Community finding (Safe Harbour) then accordingly the judicial review of the decision not to investigate must fail. He noted that the ODPC had 'demonstrated scrupulous steadfastness to the letter of the 1995 Directive and the 2000 decision'. However the Court went on to note that given the novelty and practical importance of the issues (primarily the validity of Safe Harbour) for all 28 Member States, the Court of Justice should determine whether an independent office holder such as the ODPC is absolutely bound by a Community finding or whether the office holder may conduct his or her own investigation of the matter in light of factual developments in the meantime since. At the time of writing the Court of Justice decision is pending.

LATVIA

Sarmis Spilbergs
Senior Associate
T +371 67814848
E sarmis.spilbergs@lawin.lv

On the horizon

Reporting requirements when performing duties of state administration

During 2014 we saw substantial changes in the Personal Data Protection Law (the PDPL). However, as a result of resources currently being focussed on Latvia's presidency of the Council of the European Union no major changes in the data protection landscape in 2015 are expected. One noteworthy change to the PDPL in 2014 was the requirement that not only public institutions but also private companies that have been delegated public functions must prepare a report on compliance with personal data processing requirements, including risk analysis and measures taken in the sphere of information security. The Cabinet of Ministers has developed a draft order setting out how the reporting should be done and providing a template for the report. This order is due to take effect in the second half of 2015.

Local data retention provisions under review

The Electronic Communications Law (the ECL) transposed the Data Retention Directive (2004/24/EC) in to Latvian law. Amongst other things the ECL provides for a data retention period of 18 months. Following the decision of the Court of Justice of the European Union (the CJEU) which held the Data Retention Directive to be invalid, the ECL is also potentially open to challenge on the basis of its incompatibility with an individual's human right to privacy. Since the judgment of the CJEU, Latvian authorities have met on several occasions to discuss the possible amendments to the ECL. No specific amendments have been suggested so far, but it is expected that in the second half of 2015 the authorities will either propose draft amendments to the potentially conflicting ECL rules or, depending on the data currently retained by market participants, provide a middle ground solution.

Cases

Borderline between public interest and the right to privacy

On 30 December 2014 the Ombudsman of Latvia filed an application to the Constitutional Court of Latvia regarding recent changes in the law on maintenance payments. The new law provides that, in the event where a parent fails to pay child support, the parent's personal data may be disclosed to third parties. The personal data would include the name and identity code (which also identifies the parent's birth date). There is a concern that this could violate the rights to personal and family life rather than protect the rights of the child. Moreover, disclosing personal data to the public might lead to possible identity thefts. If the Constitutional Court accepts that it will hear the application then, regardless of the ultimate ruling, the judgement of the Constitutional Court will include interpretation on such significant issues as the scope of personal data and clarity on the boundary between public interest and the right to privacy.

The scope of data protection under Latvian law

In several recent cases the interplay between an individual's right to freedom of speech and another's right to protection of personal data and privacy have been reviewed. One such case concerned filming police officers performing their duties in the premises of a state police department and publishing the video online. The author claimed that police officers should be considered state officials performing their duties in a public place and, thus, outside the scope of personal data protection. However, the Latvian Court of First Instance ruled that personal data protection also concerns situations where processing of personal data does not relate to one's private life. Moreover, according to the Court's opinion Latvian law also protects data which are not automated or contained or intended to be contained in a filing system. Thus, the scope of protection under Latvian law is broader than provided in the Data Protection Directive 95/46/EC. More developments on this case are expected later in 2015 when the applicant's appeal will be heard.

THE NETHERLANDS

VanDoorne
Advocaten • Notarissen • Fiscalisten

Elisabeth Thole
Counsel
T +31 20 6789 293
E thole@vandoorne.com

On the horizon

Data breaches and increased fine competence Dutch DPA

In February 2015 the Dutch House of Representatives agreed to a legislative proposal introducing the obligation for data controllers to notify the Dutch Data Protection Authority (the DDPA) of any data breaches without undue delay if such breach could have a severe negative impact on the security of personal data. The data subjects should also be notified if the breach is likely to have a negative impact on their privacy. In addition the legislative proposal seeks to increase the ability of the DDPA to impose administrative fines, not only for data breaches but also for other violations of the Dutch Data Protection Act. The increased fines may be imposed up to a maximum of EUR 810,000, or 10% of the annual turnover of an enterprise. It is expected that the proposal will enter into force in 2015.

Cookies

Also in February 2015, the Dutch Senate agreed to relax the Dutch cookie rules allowing website owners to place cookies that have no or only marginal impact on the user's privacy without the consent of the user. First party analytic cookies, performance or affiliate cookies may be placed without the user's consent. Cookies used to analyse the behaviour of the user over time and across a number of websites are not included in the exception and the use of such cookies is still subject to informed consent.

Debate on the retention of telecom data rules

As a result of the European Court of Justice decision of April 2014, declaring the EU Data Retention Directive to be invalid, the legislative proposal that would amend the Dutch Telecommunication Act to provide for similar data retention laws has also been subject to debate. In February 2015 the DDPA recommended that the proposal be withdrawn, as it considers that the proposal is too far-reaching. In addition certain stakeholders were sucessful in challenging the implementation act in legal proceedings against the Dutch State.

Cases

SMS parking

In August 2014 the Court of Appeal ruled that the parking company, SMS Parking, was required to provide personal data of its customers upon the request of the Dutch Tax Authority. SMS Parking had tried to argue that the Dutch Data Protection Act prevented them from providing this information but the Court disagreed. The Court of Appeal held that the general interest of levying and collecting taxes should prevail over the privacy interests of the individual data subjects.

License plate parking cases

In numerous cities in the Netherlands parking control is executed through scanning license plates. The legitimacy of this method is now being debated. In 2014 three cases were brought to court by individuals who received parking tickets. From a privacy perspective the most relevant decision was given in December 2014, where the defendant argued that scanning license plates would constitute a violation of his privacy. In its ruling the Court held that the privacy impact of this practice is limited, since only the license plates of individuals who did not pay their parking charge will be connected to an individual in order to impose fines. Because of the (efficiency) benefits this method provides, some violations of the privacy of the parker are justified.

RTBF case

The District Court of Amsterdam restrictively interpreted the Google/Costeja (RTBF) decision in two cases in September 2014 and February 2015. In both cases, the Court held that the RTBF decision aims to protect individuals from publication of information that is irrelevant, excessive or unnecessarily defamatory, and is not meant to protect individuals against all negative publication on the internet. The claims to remove information on: (a) the conviction of a murder; and (b) a dispute between a building contractor and its client, were both dismissed.

NORWAY

SCHJØDT

Jeppe Songe-Møller
Senior Lawyer
T +47 23 01 15 64
E jeppe.songe-moller@schjodt.no

On the horizon

Stricter "app" regime

The Data Protection Authority (the DPA) (the Norwegian regulator with responsibility for overseeing compliance with Norwegian data protection laws) continues its focus on privacy issues related to downloading and use of apps. Recent market searches indicate that many apps are collecting large amounts of personal data. As many as 85% of these do not explain well enough how they collect, use and delete the personal data that is collected. The DPA is particularly worried about the lack of information concerning use of smartphone sensors and sharing of personal data with third parties without prior consent. Samsung was one of seven companies which were addressed in a letter from international data protection authorities. Apple, Microsoft, BlackBerry, Google, Amazon and Nokia received a similar letter, in which they were each encouraged to take responsibility for information to consumers concerning the collection of personal data through the downloading and use of apps. The letter states that it should become mandatory for apps downloaded from different app stores to link to a privacy statement.

Heavier fines for unauthorized access to employee email

Several Norwegian companies have been fined EUR 10,000 for accessing employee emails without legal authority. The number of enquiries to the DPA about access to and deletion of employees' email accounts are increasing. Clear violations of the rules in the Norwegian Personal Data Regulations may lead to standardized fines of EUR 10,000. The majority of businesses subject to fines come from the private sector. Problems seem to occur in cases where the employee's employment has been terminated, but the employer has received automatically forwarded emails and the former employee's email account has been kept open for a while after the employment has ended.

Cases

Private camera surveillance

In its decision of 11 December 2014, the European Court of Justice (the CJEU) held that use of a surveillance camera by a private individual is not deemed as being for a purely personal or private purpose if private individuals' camera surveillance also captures a public area. Following the decision by the CJEU, the DPA issued a statement which clarifies the Norwegian position as regards private camera surveillance. The DPA stated that private individuals' camera surveillance falls within the scope of the Data Protection Directive (95/46/EC) and that such surveillance of public areas will thus be subject to the Norwegian Personal Data Act. The DPA also stated that "although the ruling in the CJEU is directed specifically against a private individual who monitors public areas, there is much to suggest that the same must apply to a private person who is monitoring a neighbour, public road or similar".

Google search removal

The DPA has ruled on three complaints from individuals following the "Google-judgment", where the CJEU held that individuals could apply to Google with the aim of being removed from the search engine result lists. The ruling gave Google and other search engines responsibility for the processing of personal data which is done when indexing websites. The ruling therefore implied a requirement for search engines to respect fundamental rights of privacy. National data protection authorities were appointed as appeal bodies to Google's own decisions regarding removal from result lists. In one of the Norwegian cases, an athlete was successful in his appeal to the DPA, and his name will therefore be deleted from the result lists. The athlete found it distressing that his name came up in the Google search results suggesting that he had tested positive for drugs. The athlete was acquitted of the charges, but this was not clear in the search results. Two of the three complaints heard to date were not successful. The DPA's assessment was that the criminal cases in question were still of public interest.

POLAND

Agnieszka Szydlik
Advocate
T +00 4782 2437 8200
E agnieszka.szydlik@wardynski.com.pl

On the horizon

New regulation on data protection officer

The amendment to the Personal Data Protection Act (PDPA) that came into force on 1 January 2015 regulates in detail the position of data protection officers (DPOs). From now on DPOs will be registered with Poland's data protection authority, the Inspector General for Personal Data Protection (the GIODO). DPOs have also gained new powers, including maintaining their own register of filing systems, which previously had been done exclusively by the GIODO.

Data controllers may, but do not have to, appoint a DPO. However, if they do appoint a DPO they must notify the details of their DPO in the register maintained by the GIODO and they generally will not be required to register their filing systems of personal data with the GIODO (with the exception of sensitive personal data).

To be eligible to serve as a DPO under the amended PDPA, a person must:

- have full legal capacity and full public rights;
- have appropriate knowledge in the area of personal data protection; and
- not have been convicted of an intentional criminal offence.

DPOs do not have to be Polish citizens.

In addition, the PDPA requires the data controller to provide the DPO with the means and organisational separation needed to perform the DPO's tasks independently - previously this was only regarded as best practice.

Registration of filing systems

The latest amendments to the PDPA have also removed the requirement for data controllers to register their filing systems with the GIODO if they do not use IT systems and/or do not contain sensitive personal data. The previous rules required data controllers to register nearly all filing systems (whether in electronic or paper form) with the GIODO, regardless of the type and the scale of operations, if the data involved did not fall within an exemption from registration (e.g. for employee data or publicly available data).

As noted data controllers who have appointed a DPO and registered the DPO with the GIODO do not have to register their filing systems with the GIODO unless they contain sensitive personal data. Instead, upon registration with the GIODO, the DPO is required to maintain a register of filing systems. If the register is maintained in electronic form, the DPO is required to provide access to the register on the website of the data controller or make it available for review to any interested person on the IT system at the data controller's registered office.

Cases

Monitoring of employees

There are no laws in Poland that directly regulate monitoring. The Supreme Administrative Court has recently considered the conditions that an employer (being a data controller) should observe to ensure the legality of monitoring. Taking the view that monitoring may be carried out by virtue of an essential need to meet the employer's legitimate objectives, the court pointed to additional conditions that ensure that the monitoring does not violate the rights and freedoms of monitored individuals. In particular, the court stated the need to inform staff of the monitoring. Employers should specify in detail the rules for monitoring and inform staff of them. Staff members should then confirm that they have read the rules by way of an appropriate statement of acceptance.

Sharing of data by internet website operators

There has been a long-running dispute over the possibility of sharing with individuals the personal details of authors of entries posted on websites. In refusing to disclose to individuals the IP addresses of devices used in posting entries concerning the requesting person, the owners of websites referred to the provisions of the Act on Providing Services through Electronic Channels, which allows information to be provided to "state organs". In a decision last year, the Province Administrative Court in Warsaw gave an interpretation of the regulations, concluding that there are no grounds for excluding individuals from the group of potential recipients of the disputed information.

PORTUGAL

PLMJ
SOCIEDADE DE ADVOGADOS, RL
A.M.PEREIRA, SÁRAGGA LEAL, OLIVEIRA MARTINS, JÚDICE E ASSOCIADOS

Daniel Reis
Partner
T +351 213 197 313
E daniel.reis@plmj.pt

On the horizon

Protection of medical information

In 2014, the Portuguese Data Protection Authority (the CNPD) delivered a document to the Portuguese Parliament which highlighted the unconstitutionality of current legislation which allows entities, for example insurance companies, access to confidential medical information.

This access is possible due to the partial overlap of two laws, the Portuguese Data Protection Law (the DPL), and the Freedom of Information Act (the FIA) which regulates access to public sector information. Contrary to what happens in the DPL, the FIA establishes more flexible requirements for accessing public sector information, which can be consulted by anyone who has a "legitimate interest" in it. This has allowed insurance companies to access medical information about the National Health Service's users without their consent, resulting not only in the violation of the DPL's provisions on sensitive personal data, but also in the inequality of the level of protection of the patients' medical information depending on whether they use public or private healthcare services. The aim is for the law to be changed during 2015 to ensure that all access to such sensitive personal data is subject to the DPL standards of protection and to the control of the CNPD.

Geolocation technology in the workplace

In November 2014, the CNPD published an opinion establishing the framework and conditions applicable to the processing of personal data collected through the use of geolocation technology in the workplace. These provisions focus on geolocation technologies used in devices made available by the employer to the employee, and particularly focussed on those used in motor vehicles and mobile devices, such as mobile phones, tablets and laptops.

Following this opinion, placing geolocation devices in motor vehicles is allowed for specific purposes only. In addition, the use of geolocation technology to monitor an employee's professional performance or to monitor employees during their free time is strictly prohibited.

These provisions also introduce new information obligations: the employers are required to notify the employees of the use of geolocation devices and to inform them, in writing, of the conditions of and restrictions on use of any relevant equipment. Furthermore, the processing of employees' geolocation data is subject to prior authorisation by the CNPD. The impact of these new rules will begin to be felt during 2015.

Cases

"Secretas" case

In 2014, the CNPD imposed a fine of EUR 4,5 million on Optimus, a Portuguese telecommunications operator, due to the infringement of data protection provisions. It was the largest penalty ever imposed by the CNPD.

The facts date back to 2010, when an Optimus employee delivered the communication records of a journalist's mobile phone to an officer of the Defence Strategic Intelligence Service (part of the Portuguese Secret Services known as "Secretas") who was trying to discover the journalist's information source, because the journalist had released some classified information.

Optimus was found guilty of four offences: the lack of adequate measures to control data access by its employees; non-compliance with the data storage requirements; retention of data beyond the required time for retaining traffic data; and the failure to reconcile the rights of subscribers and the users' privacy.

However, the telecommunications operator appealed to the Competition, Regulation and Supervision Court, which reduced the fine to EUR 600,000. Optimus then appealed again to the Court of Appeal of Lisbon, which issued the final decision in February 2015, setting the fine at EUR 100,000, as it considered that only one of the offences was proven (the fact that too many employees had access to the call records of customers, due to the lack of control measures).

SPAIN

GARRIGUES

Alejandro Padín Vidal
Counsel
T +34 91 514 52 00
E alejandro.padin@garrigues.com

On the horizon

Data retention

In a recent ruling, the Madrid Court of Appeal (Audiencia Provincial) looked at the definition of 'serious crimes' as set out in the Spanish Data Retention Act (the DRA). The Audiencia Provincial noted that the DRA defines 'serious crimes' in very broad terms, since it does not lay down any objective criterion to identify them and, for instance, does not specify when a case would fall within its scope or not. It was such lack of legal certainty in the Data Retention Directive (2006/24/EC) (from which the DRA is derived) which caused the Court of Justice to hold the Directive invalid in April 2014. The Audiencia Provincial was forced to interpret what the DRA meant by "serious crimes", finally deciding that the measures introduced by the DRA could be applicable, in certain cases, even where the applicable penalty is less than five years' imprisonment (not normally classed as a "serious" offence in Spain). This controversial ruling is likely to reopen the discussion about whether the DRA should be repealed, which could be achieved either through a Parliamentary decision or through a decision of the Constitutional Court, if a particular case ends up reaching that jurisdiction.

Cookies and marketing activities

The Spanish Telecommunications Act 9/2014 has amended article 37 of the Information Society Services and Electronic Commerce Law (known in Spain as the "LSSI") which deals with infringement of the laws relating to cookies. The new provision means that an advertising network or agent could also be subject to penalties in certain cases, alongside the information society service provider. This is particularly likely to arise where the advertising network or agent has arranged directly the placing of adverts in spaces of the service provider, and the advertising network or agent have taken no steps to ensure that the information society service provider is complying with the cookies legislation, provided that the infringement arises because of cookies that have been placed as a result of the advert. Potential penalties arising from unlawful processing of cookies are subject to a maximum of €150,000 under the LSSI and up to €300,000 under data protection legislation. This new regulation has been met with astonishment by the advertising and marketing sector (advertisers, agents, editors) as in many cases it is very difficult for them to ensure that internet service providers implement the cookies rules.

Cases

Right to be forgotten – not forgotten by the Court

Following the famous 'Mario Costeja vs. Google Inc.' judgement of the Court of Justice (ECJ), the National Central Court (Audiencia Nacional) finally ruled on the Spanish case that originated the 'right to be forgotten' preliminary ruling. On 29 December 2014, this Audiencia Nacional followed the criteria established by the ECJ in order to exercise the right to object before the data controller or the Spanish Data Protection Agency (DPA). According to the ruling, the data subject must bring evidence that the search has been undertaken using his personal name, and must show the list of links obtained through the search engine, as well as the information which could be accessed through those links, implying the treatment of his personal data. The data controller (or DPA, as the case may be), under the final control of the courts, shall decide whether to accept the claimant's position or not on a case by case basis, taking into account the balancing of the rights at stake and the personal situation of the data subject, along with the nature of the information and its sensitivity, as well as the time elapsed since the data was created.

Data protection and telecoms regulation

Although not quite so recent, at the end of 2012 the DPA ruled on an interesting case which saw them consider the balance between the data protection principles and telecommunications regulation principles. In this case certain telecoms operators had filed a complaint against some app developers who were using public information about the portability of cell phone numbers which they had obtained from the website of the Spanish Telecoms Market Commission (CMT). Paradoxically the DPA ruled in favour of the app developers basing their reasoning on the superior status of the telecommunications laws principles stated in the EU Directives and the Spanish Regulation. Does this open the door for new services?

SWEDEN

Peter Nordbeck
Partner
T +468 677 5530
E peter.nordbeck@delphi.se

On the horizon

During 2014 the Swedish Data Inspection Board (the DIB) handled a number of interesting supervision matters involving personal data processing in health care, such as direct access to patient records and cloud services, as well as issues arising from various types of registers within the public sector, for example, the Swedish police's criminal and surveillance register and registers kept by the Bolagsverket (the Swedish Company register) and Domstolsverket (the Swedish courts administration).

There are currently a number of ongoing public reviews and proposals for new legislation related to data protection, one of which relates to permitting so-called register-based research. If the proposed legislation is enacted this would permit authorities which maintain such registers to disclose information to those creating research databases. The DIB is critical of this proposal, one reason being that it allows for an intimate mapping of individual privacy, family circumstances, medical history, employment and crime data without informing the individuals that the data is being collected.

Another ongoing review in Sweden is specifically focused on the regulation of personal data processing by public authorities. The scope of this review was revised in May 2014 in order to be better adapted to the upcoming General Data Protection Regulation (the GDPR). The results of the review are due to be presented in Spring 2015.

Sweden's view on the GDPR

Since January 2012 when the Commission presented its proposal for a new GDPR the proposal has been discussed and debated extensively by EU legislators. Sweden maintains the view that the new rules on data protection should be adopted as a directive instead of a regulation in order to allow more flexibility for national sector-specific regulations such as the Swedish principle of public access to official records (Sw: offentlighetsprincipen). Sweden is also promoting that the GDPR adopts a so called risk-based approach similar to the current Section 5a of the Swedish Personal Data Act.

At the Council meeting on December 4 2014, a proposal for the applicability of the GDPR to the public sector was discussed and adopted (as a temporary partial – non-binding – agreement). Prior to that meeting the Swedish Department of Justice had presented some additional comments on the GDPR and expressed that Sweden was positive about the latest proposal because, amongst other things, greater influence is given to national laws dealing with the public sector and because the Swedish principle of public access to official records appears to be taken into account.

SWITZERLAND

walderwyss attorneys at law

Jürg Schneider
Partner
T +41 58 658 58 58
E juerg.schneider@walderwyss.com

On the horizon

Planned reform of the Swiss Data Protection Act

In 2011, a group of researchers led by the Swiss Federal Office of Justice carried out an evaluation of Swiss data protection laws. This evaluation has revealed the need for a reform of the Swiss Data Protection Act (the DPA). In particular, according to the evaluation report, ongoing technological and social development constitutes a threat to data privacy, which the current DPA can no longer contain adequately. The main risks for data privacy identified are the growing amount of personal data being transferred abroad and the lack of control over personal data which has been disclosed to third parties. Based on more detailed proposals for reform elaborated by a working group nominated by the Swiss Federal Department of Justice and Police (FDJP), the Swiss Federal Council formally decided to undertake a revision of the DPA on 1 April 2015. The Swiss Federal Council has instructed the FDJP to submit a preliminary draft for a revision of the DPA by the end of August 2016 at the latest.

With this reform, the Swiss Federal Council intends to lay the foundations which will allow Switzerland to ratify the modernised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and, to the extent this is necessary in the context of further development of the Schengen/Dublin acquis, the adaptation of the DPA to the EU data protection provisions.

During the course of the development of the preliminary draft, a strengthening of the position and competencies of the Swiss Federal Data Protection and Information Commissioner (the Commissioner) and of the enforcement rights of data subjects shall be considered. According to the Swiss Federal Council, the reform shall also improve data control and data ownership as well as the protection of minors. Finally, strengthening rules of good practice shall ensure that data protection becomes effective at an earlier stage.

Further ongoing reforms concerning privacy issues

The Swiss Parliament is currently discussing a new law on electronic files for patients which will establish the legal basis for the maintenance of electronic medical files.

Also under review is the Swiss Act on the Supervision of Postal and Telecommunication Services and the Act regarding Intelligence Services ("Nachrichtendienst"). The amendments being proposed to the latter are expected to increase the scope for surveillance of individuals, in particular in connection with the prevention of terrorism, and have been criticised as undermining privacy and other fundamental rights.

Finally, the Swiss legislation dealing with the Commercial Register (the register of companies) is currently being updated. As part of that particular reform the Swiss Parliament has decided that no "right to be forgotten" shall be introduced with respect to commercial register data.

Work of the Commissioner

In 2014 one main focus of the Commissioner was a review of data privacy issues arising in connection with customer cards used by food retailers in Switzerland and privacy issues in connection with internet information platforms. The Commissioner is particularly concerned with the establishment and processing of so-called "personality profiles". A personality profile is a collection of data that permits an assessment of essential characteristics of the personality of a natural person (such as credit or customer card data revealing travel or shopping patterns; equally, e.g. HR files, medical data files and data pools of insurance companies may contain personality profiles). Personality profiles benefit from an increased level of protection in Switzerland similar to sensitive personal data.

In 2014, the Commissioner also published several new guidelines, in particular regarding the right to be forgotten, tracking of persons, publishing of photos and video surveillance with drones

Cases

In terms of court decisions, the Swiss Federal Supreme Court (the Court) decision of 12 January 2015 in connection with the tax dispute between certain Swiss banks and the US is particularly noteworthy. Based on the right of access set forth in the DPA, the Court obliged a Swiss bank to provide its employees with copies of all documents transferred to the US Department of Justice (DoJ) in April 2012 containing their personal data [1].

1.Federal Supreme Court decisions dated 12 January 2015, 4A_405/2014; 4A_408/2014.

UK

SHEPHERD+WEDDERBURN

Nicola Rinaldi
Associate
T +44 (0)131 473 5466
E nicola.rinaldi@shepwedd.co.uk

On the horizon

Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)

The Information Commissioner's Office (the ICO) (the UK regulator with responsibility for overseeing compliance with UK data protection laws) had encountered difficulties over the last couple of years in imposing fines for failures to comply with PECR, failures such as the making of unsolicited calls and the issuing of unsolicited SMS text messages. The difficulty arose because in order to levy a fine for a breach of PECR, PECR required that the offending calls and/or messages must cause or be likely to cause 'substantial damage or substantial distress'. It had been held that this test is not satisfied merely because a large number of calls or messages had been made or sent. However, as of 6 April 2015 the legal threshold has been lowered so that all that has to be established is that the offending party committed a serious breach of PECR. This change to the law will make it easier for the ICO to take enforcement action against those making of unsolicited calls and those sending mass mailings of spam texts and/or emails.

Judicial Review of Data Retention and Investigatory Powers Act (DRIPA)

In July 2014 the UK government controversially rushed DRIPA into law. DRIPA was intended to fill the gap caused by the European Court of Justice (CJEU) holding that the Data Retention Directive 2006/24/EC (and by extension local legislation based on that Directive) was invalid. DRIPA requires internet and phone companies to collect their customers' personal communication data, tracking their phone and internet use, and store it for 12 months to give access to the police, security services and up to 600 public bodies on request. DRIPA is itself now being challenged on the grounds that it is incompatible with human rights law as it violates an individual's fundamental human right to privacy (the same argument made in the CJEU in respect of the Data Retention Directive). The date for hearing is likely to be set in 2015.

Cases

Is a name personal data?

In the UK there has, for many years, been much discussion and confusion as to what constitutes "personal data" and in particular whether a name of itself can be personal data. In the leading case on the issue the court held[i] that the mere mention of a person's name in a document does not make that whole document available as "personal data" and this seemed to many to suggest that a name in and of itself would not be personal data.

In the Efifiom Edem[ii] case, however, the Court of Appeal concluded that 'a name is personal data unless it is so common that without further information, such as its use in a work context, a person would remain unidentifiable despite its disclosure'. The court also said that it is not always necessary to consider the biographical significance of information in determining whether it qualifies as personal data. Although this provides important clarification many questions as to the extent of the definition of personal data remain.

Compensation

One of the difficulties for data subjects in the UK is that it has been assumed that compensation for distress caused by a breach of the Data Protection Act 1998 can only be awarded where the data subject has also suffered some form of financial loss. The UK courts are now starting to show that they are willing to award nominal amounts of damages in order to allow them to make awards for distress suffered. In the most recent case[iii] the court awarded nominal damages of £1 and then compensation for distress arising out of a failure to deal properly with a subject access request at £2250. However, the Court of Appeal[iv] has considered whether it is in fact necessary to establish financial loss at all before an award of compensation is made and held that compensation would be recoverable under s.13(1) for any damage (whether pecuniary damage or non-pecuniary damage) suffered as a result of a contravention by a data controller of any of the requirements of the DPA. As a result of the outcome of this case, we may see many more such claims for compensation in the future.

---

i. Durant v Financial Services Authority [2003] EWCA Civ 1746
ii. Efifiom Edem v The Information Commissioner and The Financial Services Authority [2014] EWCA Civ 92
iii. AB v Ministry of Justice [2014] EWHC 1847 (QB)
iv. Vidal-Hall and Others v Google Inc. [2015] All ER (d) 307 (Mar)

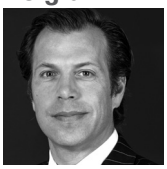
UK

Nicola Rinaldi
Associate
T +44 (0)131 473 5466
E nicola.rinaldi@shepwedd.co.uk

Austria

Axel Ander
Partner
T +431 533 479 523
E axel.anderl@dbj.at

Belgium



Gerrit Vandendriessche
Senior Partner
T +322 426 1414
E gerrit.vandendriessche@altius.com

Czech Republic

Drahomir Tomasuk
Counsel
T +420 224 103 316
E dtomasuk@ksb.cz

Denmark

Michael Hopp
Partner
T +453 694 1306
E mho@plesner.com

Estonia

Pirkko-Liis Harkmaa
Associate Partner
T +372 630 6460
E pirkko-liis.harkmaa@lawin.ee

Finland

JP Alho
Partner
T +3582 9000 6264
E jp.alho@krogerus.com

France

Isabelle Pontal
Counsel
T +33 01 45 05 81 05
E ipontal@jeantet.fr

Germany

Astrid Luedtke
Lawyer
T +49211 600 55 168
E a.luedtke@heuking.de

Hungary

Dr. László Pók
Partner
T +361 472 3000
E laszlo.pok@szecskay.com

Ireland

Mark Rasdale
Partner
T +353 1649 2300
E mrasdale@algoodbody.com

Latvia

Sarmis Spilbergs
Senior Associate
T +371 67814848
E sarmis.spilbergs@lawin.lv

The Netherlands

Elisabeth Thole
Advocate
T +31 20 67 89 293
E thole@vandoorne.com

Norway

Jeppe Songe-Møller
Senior Lawyer
T +47 23 01 15 64
E jeppe.songe-moller@schjodt.no

Poland

Agnieszka Szydlik
Advocate
T +00 4782 2437 8200
E agnieszka.szydlik@wardynski.com.pl

Portugal

Daniel Reis
Partner
T +351 213 197 313
E daniel.reis@plmj.pt

Spain

Alejandro Padín Vidal
Counsel
T +34 91 514 52 00
E alejandro.padin@garrigues.com

Sweden

Peter Nordbeck
Partner
T +468 677 5530
E peter.nordbeck@delphi.se

Switzerland

Juerg Schneider
Partner
T +41 58 658 58 58
E juerg.schneider@walderwyss.com

CF30 24103/15