TILBURG LAW SCHOOL
LEGAL STUDIES RESEARCH PAPER SERIES

Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges

Monika Kuschewsky
Covington & Burling
mkuschewsky@cov.com

&

Damien Geradin
Tilburg University
tilburguniversity.edu

Tilburg Law School Legal Studies Research Paper Series
No. 020/2013

Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges

Monika Kuschewsky and Damien Geradin[(*)]

I. Introduction

The interface between data protection law and competition rules has become a growing area of interest for companies and lawyers. First, in the course of unannounced inspections (the so-called "dawnraids"), European Commission (the "Commission") and national competition authority officials typically review company records and search employees' e-mails and electronic files and records (including those which people thought had been deleted). They will make hard and/or soft copies of relevant documents and in certain cases may even seize entire hard discs. This raises the question of whether such intrusions are compatible with data protection rules and thus which restrictions such rules impose on the ability of competition officials to collect and process data seized during inspections. Another intersection between competition law and data protection law arises where companies need to collect and further process data from their employees to respond to a competition authority's request for information or a statement of objections in the course of a pending competition law investigation. Companies may also wish to access and review e-mails and other employee records so as to uncover potential competition law infringements (e.g., in the context of a compliance programme) or to prepare a leniency application.

This paper seeks to identify the limits that may be placed by data protection law on competition authorities, on the one hand, and companies, on the other hand, to collect and further process personal data in the context of competition law investigations.

The potential conflict between competition and data protection rules has come to the fore because of the increase in the sheer volume of data following the advent of automatic processing, cheaper storage capacities and the development of electronic means of communication. As a consequence, competition law investigations have become increasingly data intensive. At the same time, various types of software allow searching larger volumes of data in a much shorter time period. The use of forensic data analytics in competition law investigations is also on the rise, for instance, to analyse data, map

[(*)] Monika Kuschewsky is a Special Counsel at Covington & Burling (mkuschewsky@cov.com). Damien Geradin is a partner at Covington & Burling, a Professor of Law at George Mason University School of Law and a Professor of competition law & economics at Tilburg University (dgeradin@cov.com).

individual trends, compare different data sets to establish the likelihood of the existence of an infringement or to quantify the potential impact of a purported infringement on the market.[1]

Documents, files and other records – whether stored electronically on a server, a computer or a mobile phone, or physically in a cupboard or paper archive – gathered in cartel or abuse of dominant position investigations will frequently contain personal data relating to employees of companies that are subject to an investigation or of third parties, including suppliers, customers or competitors. Collecting, accessing, and reviewing these records constitutes data processing, thus triggering the application of data protection law.

In the European Union ("EU"), data protection rules apply to public authorities, including competition authorities at EU and national level, and companies.[2] Although both are in essence subject to the same data protection principles, competition authorities usually have broad powers of inspection[3] and can benefit from a number of exemptions from certain key principles of data protection law, which makes it easier for them to comply with data protection rules. By contrast, data protection rules will hit private organisations with their full power. Unless companies put in place procedures and other safeguards to address data protection law requirements before an issue arises, the data protection rules may severely affect the ability of companies to proactively detect competition law infringements and collect the relevant evidence. It can also cause considerable delays, which is a serious problem as time is of essence when replying to a request for information, but also in the race to leniency when a cartel is uncovered.

Even if this double standard may be justified, it arguably leads to an information asymmetry, and thus an inequality of arms, between competition authorities and

---

[1] Muthmainur Rahman and Matt Rees, "Analysing the information - Data analytics has an important role to play in competition cases", *Competition Law Insight*, 19 March 2013. For another example, see "Research firm should reveal cartel data, Dutch appeal court rules", *MLex*, 13 June 2013, where the Dutch competition authority reportedly requested a research company hired by a suspected cartelist to retain documents which the company had obtained for the purposes of performing digital forensic research and to disclose the names of all the companies in the sector that had requested similar services.

[2] There is a proliferation of data protection laws worldwide. Although official figures are not available, the number of countries with data protection laws is steadily growing. The June 2013 Privacy Laws & Business International Report lists 99 countries with data protection laws..

[3] The General Court just recently discussed the Commission's powers regarding inspections and rejected Deutsche Bahn's application for annulment, see Judgment of the General Court (Fourth Chamber) of 6 September 2013, *Deutsche Bahn AG and Others v European Commission*, Joined cases T-289/11, T-290/11, T-521/11, available at: http://curia.europa.eu.

companies when it comes to the gathering and subsequent processing of relevant information in the context of competition law proceedings.[4]

This paper is divided into four sections. Section II briefly sets out the legal framework for data collection and processing in the EU. Section III explains the key data protection principles and Section IV identifies the key players in the context of EU data protection law. Section V elaborates on the key data protection principles and how they apply to competition authorities on the one hand and companies on the other hand. Section VI discusses the legal consequences of non-compliance with data protection rules. Section VII concludes.

II. The EU Data Protection Legal Framework: Setting the Stage

In the spring of 2010, the President of the Versailles Court of Appeal in France held that the seizure of the entirety of the e-mails of a company's employees during an inspection by the French competition authority in connection with a suspected abuse of dominance did not violate the company's procedural rights.[5] In particular, the Court argued that any obligation to exclude private e-mails from the seizure would severely hinder the reliability of the information retrieved, that the documents in question were not marked as private and the company did not object, at the time, to the seizure of the e-mails. In November 2011, this judgment was upheld by the French Supreme Court, which ruled that data protection law is not applicable in the event of a seizure taking place in the framework of an inspection that was authorised by a judge.[6] The simple fact that an e-mail account contains, even if only partly, elements falling within the scope of the authorisation would be sufficient to allow seizure of the e-mails in their entirety.

These rulings suggest that competition authorities fall outside the remit of data protection law. This is a misconception as competition authorities in the EU are generally subject to the same basic data protection principles that apply to companies. In fact, the

---

[4] For a discussion of the constraints imposed on the Commission's powers by the right to privacy and the problems in the Commission's practice, see John Temple Lang, "Legal Problems of Digital Evidence", *Journal of Antitrust Enforcement*, August 2013.

[5] Cour d'appel de Versailles, order (Ordonnance) of 19 February 2010, *Janssen-Cilag*, available at: www.legalis.net.

[6] Cour de cassation (Crim.), 30 November 2011, No 10-81.748, available at: www.legifrance.gouv.fr; see also Olivier Proust, "French Court of Appeals Ruling Upholding Competition Authority's Search and Seizure Of Company Employees' Emails", 10(5) *BNA World Data Protection Report* 1.

Commission (DG Competition) has explicitly acknowledged that it is subject to data protection law.[7]

The two relevant legal instruments at EU level are Regulation (EC) No 45/2001 (the "Regulation")[8] and Directive 95/46/EC (the "Data Protection Directive"),[9] which are both based on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the "Convention 108"),[10] adopted by the Council of Europe in 1981. The Regulation aims to protect personal data processed by EU institutions and bodies in the exercise of activities within the scope of EU law. It thus applies to the Commission, including DG Competition. The Data Protection Directive, which has been implemented by all members of the European Economic Area (the "EEA"), lays down the legal framework for the processing and transfer of personal data by both public authorities at EEA Member State level (including national competition authorities) and companies. This dichotomy of legal frameworks is unlikely to disappear in the near future. While the Data Protection Directive is currently undergoing a reform, the Commission has not proposed any changes to the aforementioned Regulation.[11]

III. Key Data Protection Notions Competition Lawyers Should Keep in Mind

The two key data protection notions are "personal data" and "processing".

---

[7] See Explanatory note to an authorisation to conduct an inspection in execution of a Commission decision under Article 20(4) of Council Regulation No 1/2003, as revised on 18/03/2013, para. (18), available at: http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf: "*Any personal data, as defined in Regulation No. 45/2001 in documents copied or obtained during the inspection will be processed in compliance with that Regulation*."

[8] Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L8/1, 12 January 2001.

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23 January 1995.

[10] Convention 108 of 28 January 1981 is the first legally binding international instrument in the field of data protection, which guarantees the protection of personal data as a separate right granted to individuals. Before that, at European level, the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, which entered into force in 1953, ensured the respect for private life.

[11] See Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "proposed GDP Regulation"), COM/2012/011 final, and Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM/2012/010 final, both published in January 2012.

Personal data is defined as

> "any information relating to an identified or identifiable natural person".[12]

This, for instance, covers e-mail addresses, certain Internet logs, as well as persons' names in meeting minutes.[13] A sub-category of personal data, the so-called *sensitive data* or special categories of data,[14] is considered to be worthy of higher protection and is therefore subject to a set of stricter rules. Competition law investigations will not typically involve sensitive data.[15] However, there may be exceptions depending on the industry sector concerned (e.g., health, insurance).

Processing is defined very broadly as

> "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".[16]

In other words, processing covers the whole life cycle of personal data from collection to deletion and data protection rules must therefore in principle be respected throughout all stages of an investigation.

EU data protection law applies whenever there is electronic (or so-called automatic) processing of personal data, for instance, by means of computers. Paper files are also caught, if they satisfy the definition of a *filing system* or are intended to form part of such

---

12 Article 2 (a) of the Data Protection Directive and Article 2 (a) of the Regulation.

13 Case C-28/08 P *Commission* v *The Bavarian Lager Co. Ltd.* [2010] ECR I-6055.

14 Article 8 of the Data Protection Directive and Article 10 of the Regulation. This comprises personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, data relating to offences, criminal convictions or security measures and possibly to administrative sanctions or judgments in civil cases as well as a national identification number or any other identifier of general application.

15 In some countries, individuals may be subject to administrative or criminal sanctions for cartel law infringements and some national data protection laws qualify the fact that an individual is being suspected of having committed an offence as sensitive data. One may therefore consider whether the collection of incriminating evidence in a competition law investigation should be subject to the stricter rules applicable to sensitive data.

16 Article 2 (b) of the Data Protection Directive and the Regulation respectively.

a filing system, such as personnel files or card-index systems.[17] Although most traditional business documents and files which are of interest in a competition investigation typically do not qualify as a filing system, data protection law would apply if they are scanned in or otherwise electronically stored (provided they contain personal data).

IV. Key Players on the Data Protection Stage

The four key players when it comes to data protection are: controllers, processors, data subjects and supervisory authorities.

A. Controllers

The controllers are ultimately responsible for the lawfulness of the data processing and liable for any violation of the applicable data protection rules. The Data Protection Directive defines *controllers* as

> "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[18]

Typically, the employer is the controller of its own employees' personal data or a company of its customers' personal data, although there may be instances where this determination is more complex (such as in the case of centralised processing by shared service centres, outsourcing, etc.). It is important to note that the parent company is not necessarily the controller of all the personal data processed by individual companies of the group. This is because the controller is defined on a legal entity basis and not on a group wide basis. The determination of who acts as a controller is not only relevant for the allocation of responsibility and liability, but also determines the applicable national data protection law and the competent supervisory authority both in relation to controllers established within the EU and outside the EU.

The Regulation defines the notion of controller in a similar manner, namely as

---

[17] Article 2 (c) of the Data Protection Directive and the Regulation respectively. The Data Protection Directive defines a personal data filing system as "*any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis*".

[18] Article 2 (d) of the Data Protection Directive.

> "the Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data."[19]

For dawn raids and subsequent cartel or abuse investigations, the controller will typically be DG Competition or the relevant unit handling the case within DG Competition.[20]

B. Processors

Controllers may carry out the data processing themselves or entrust the processing activities to an entity, which processes the personal data on their behalf and under their instructions. For instance, a company may store its databases on a server in-house or alternatively on a server hosted by an external service provider, which will act as a processor. Other examples of processors, especially relevant in the context of investigations, include external service providers in charge of digital evidence gathering and filtering. Competition authorities can also make use of such service providers. In practice, this is only done rarely as competition authorities usually have their own investigation and forensics teams or trained staff.[21]

The controller must select a processor that provides sufficient guarantees in terms of security. The controller also has to conclude a processor agreement, subjecting the processor to the controller's instructions and obliging the processor to implement specific security measures.[22]

C. Data Subjects

Data subjects are the individuals whose personal data is being processed, such as employees. They enjoy certain rights under data protection law, which they may enforce by judicial remedy, and may claim compensation in case of their violation.

---

[19] Article 2 (d) of the Regulation.

[20] Rather than DG Competition's specialised unit (the Forensic IT group) dealing with digital evidence gathering.

[21] Anti-Cartel Enforcement Manual, ICN, March 2010 (infra fn. 28) - Chapter Digital Evidence Gathering, section 6.2, available at: http://www.internationalcompetitionnetwork.org/uploads/library/doc627.pdf.

[22] Article 17 of the Data Protection Directive and Article 23 of the Regulation (which reinforces the obligations of controllers vis-à-vis processors and provides for a minimum content of processor agreements).

D. Supervisory Authorities

At national level, the data protection law is enforced by the competent supervisory authorities (also called data protection authorities) that each EU Member State has to set up under the Data Protection Directive. Pursuant to the Data Protection Directive, the supervisory authorities must be endowed with investigative powers, effective powers of intervention and the power to engage in legal proceedings. In practice, there is an enormous variation in the powers of these authorities, depending on the national data protection law. In order to address this fragmentation, the proposed GDP Regulation provides for the same effective powers of supervisory authorities, including powers of investigation, legally binding intervention, decision, sanctions and to engage in legal proceedings.

At EU level, the European Data Protection Supervisor (the "EDPS") is the independent supervisory authority entrusted with the task of ensuring that the Regulation is being complied with. The EDPS can carry out investigations and has the power to warn or admonish the controller, order that requests to exercise rights be complied with, order the rectification, blocking, erasure or destruction of data and impose a ban on processing.[23]

V. The Key Data Protection Principles

The key data protection principles that DG Competition, national competition authorities and companies must comply with concern the following issues:[24] lawfulness of processing; data quality; information to be given to the data subjects; rights of the data subjects; confidentiality and security of processing; registration; and international data transfers. However, as will be explained below, due to their enhanced powers and the exceptions applicable to them, it is generally easier for competition authorities to comply with these principles than it is for companies.

At the outset, it should be noted that data protection law has not been drafted with competition law investigations in mind. The Data Protection Directive does not contain any competition law-specific rules. Rather, it is based on broad principles, which are at times difficult to apply in the context of investigations.

---

[23] Article 47 of the Regulation.

[24] For a more detailed discussion of the applicable data protection rules in the framework of corporate investigations in the private sector, see Dan Cooper, "Corporate investigations and EU data privacy laws: what every in-house counsel should know", 8(12) *BNA World Data Protection Report* 21.

Moreover, guidance on the application of the data protection rules in the context of (cartel or abuse of dominance) investigations is rather limited. The EDPS considers issuing a prospective opinion on the integration of data protection in other EU policy areas, such as competition and trade, in the second half of 2013.[25] DG Competition has published a Privacy Statement on its website, which explains in broad terms how it intends to apply the Regulation's principles to the processing of personal data in the context of its antitrust investigations.[26] The Anti-Cartel Enforcement Manual[27] issued by the Cartel Working Group of the International Competition Network (the "ICN")[28] also sheds some light on existing approaches to digital evidence gathering among competition authorities and the use of digital evidence in the context of the investigation, adjudication or prosecution of cartels, stating that:

> "It is good practice to have a systematic approach for the review, selection and handling of privileged and **private** and potentially privileged and private **digital information**."[29] (emphasis added)

DG Competition's Antitrust Manual of Procedures addresses some data protection issues in later stages of the proceedings following an investigation.[30]

As regards the private sector, guidance issued by data protection authorities regarding competition law investigations or corporate investigations has been equally sparse or non-existent. However, it is to some extent possible to extrapolate and borrow from the guidance issued by the supervisory authorities and, in particular, the Article 29 Data

---

[25] EDPS, Inventory 2013, *A strategic approach to legislative consultation*, 18 January 2013. The EDPS has also issued a number of opinions on the application of data protection rules in the context of other types of investigations. These opinions are available at: https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/OpinionsC.

[26] Available at: http://ec.europa.eu/competition/contacts/ps_antitrust.pdf.

[27] See the Chapter on *Digital Evidence Gathering*, March 2010.

[28] The ICN is an informal network of more than 100 antitrust agencies with the common aim of addressing practical antitrust enforcement and policy issues. Its work takes place in working groups, with members and nongovernmental advisors. The ICN has produced a series of practical recommendations and other tools on best practices, investigative techniques and analytical frameworks.

[29] Section 8.3.

[30] In relation to Drafting of Statement of Objections, Chapter 11, Access to File and Confidentiality, Chapter 12, and Publication of Decisions, Chapter 28. Available at: http://ec.europa.eu/competition/antitrust/antitrust_manproc_3_2012_en.pdf

Protection Working Party (the "Working Party")[31] on related areas, such as employee monitoring and surveillance, whistleblowing and e-discovery.[32]

A. Lawfulness of Processing

All data processing must be based on one of the legal grounds that make such processing legitimate. These grounds are listed in the Data Protection Directive or, in case of DG Competition, in the Regulation.[33] For instance, the necessity to comply with a legal obligation or to perform a contract, as well as unambiguous consent granted by the data subject(s) are legal grounds for data processing that can be found in both legal instruments. In order to be considered as lawful, the data processing must also respect all other applicable laws, such as labour law, including rules on works councils, telecommunications and interception laws, etc.

At the fact-gathering stage, DG Competition and the national competition authorities will usually be able to rely on their extensive powers of inspection as a legal basis for the data gathering and viewing. The Commission is empowered, among other things, to examine the books and other records of investigated companies, irrespective of the medium on which they are stored, as well as to take or obtain, in any form, copies of or extracts from such books or records.[34] National competition authorities in the EU have similar powers under their respective national laws.[35]

---

[31] This Working Party was set up under Article 29 of the Data Protection Directive. It is an independent European advisory body on data protection and privacy, comprised of a representative of the supervisory authorities of all EU Member States, as well as of the EDPS and the Commission.

[32] Working document on the surveillance of electronic communications in the workplace (WP 55), adopted on 29 May 2002; Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime (WP 117), adopted on 1 February 2006; Working Document 1/2009 on pre-trial discovery for cross border civil Litigation (WP 158), adopted on 11 February 2009. The Working Party opinions are available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/.

[33] Article 7 of the Data Protection Directive and Article 5 of the Regulation. A narrower list of legal grounds applies to the processing of sensitive data (Article 8 of the Data Protection Directive and Article 10 of the Regulation).

[34] Article 20 of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles [101] and [102] of the Treaty, OJ L1/1, 4 January 2003 (the "Regulation 1/2003").

[35] For instance, in France: Articles L450-1 to L450-8 of the French Commercial Code; and in Germany: Articles 57- 59 of the Act against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen*) (the "GWB"). For the extensive powers and the inspection practice of the German Federal Cartel Office, see Michael Saller, "Digital Evidence Gathering in German Cartel Investigations", [2013] 34 *E.C.L.R.*, Issue 2.

In subsequent stages of an investigation, the competition authorities will usually be able to rely on the so-called "*public interest*" criterion as a legal basis for data processing. In essence, this criterion allows processing that is necessary for the performance of a task carried out in the public interest or in the legitimate exercise of official authority.[36] Arguably, storing and reviewing records seized during an investigation is necessary for the Commission to perform its task of detecting competition law infringements in breach of Articles 101 and 102 of the Treaty on the Functioning of the European Union (the "TFEU") and putting them to an end.[37]

Private organisations, however, have to rely on other, less straightforward, legal bases for their data processing, which are often more difficult to satisfy.[38] Depending on the type of investigation and the surrounding circumstances, which require a case-by-case analysis, the following legal bases will typically be considered.

1. Consent

Private organisations often try to rely on the consent of the data subjects concerned in order to justify data processing in the context of investigations.[39] However, reliance on consent is usually not the best approach for several reasons. First, it is often questionable whether consent given by employees is valid. The Data Protection Directive defines consent as

> "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[40]

"Freely given" is interpreted as providing genuine choice to say "yes" or "no". This basically rules out the possibility to rely on employees' consent in most cases. The

---

[36] Article 5 (a) of the Regulation and Article 7 (e) of the Data Protection Directive.

[37] See Article 105(1) of the Treaty on the Functioning of the Union, OJ C 326, 26 October 2012, which states that "[w]*ithout prejudice to Article 104, the Commission shall ensure the application of the principles laid down in Articles 101 and 102*.", as well as recital 26 and Articles 20-21 of Regulation 1/2003.

[38] Intra-group data transfers must also be based on one of the legal grounds for making data processing legitimate. Similarly, the Regulation restricts the possibility to transfer personal data within or between EU institutions or bodies (Article 7) and to other recipients (Article 8).

[39] Article 7 (a) of the Data Protection Directive.

[40] Article 2 (h) of the Data Protection Directive.

employment relationship is characterised by the employees' subordination and employees may face adverse consequences in case they withhold consent.[41] Second, individuals are entitled to withdraw their consent at any time, rendering any subsequent processing of the relevant data unlawful. Consent must also be informed and specific. As it is necessary to specify the exact purpose of the processing, blanket consent cannot usually be validly obtained. Finally, consent would need to be obtained from all data subjects whose personal data are going to be processed within the context of an investigation. Beyond a company's own workforce and employees, this may include former employees as well as employees of customers, suppliers, competitors, etc. Obtaining consent from all these individuals will in most cases be impractical if not impossible or take considerable time.

2. Compliance with a Legal Obligation

Companies can process personal data if it is necessary to comply with a legal obligation to which the controller is subject.[42] This legal ground may be applicable, for example, if certain documents or e-mails have to be produced in response to a mandatory request for information or a court order.[43] It should be noted, however, that a foreign legal statute or regulation does not usually qualify as a legal obligation by virtue of which data processing in the EU would be legitimate.[44] This legal basis would also not apply to investigations carried out as part of a compliance programme or for the preparation of a leniency application.

3. Legitimate Interest

The legal basis most commonly invoked by companies in the context of investigations is the *legitimate interest* criterion.[45] It allows processing that is necessary for the purposes

---

41 Working Party Opinion 15/2011 on the definition of consent (WP 187), adopted on 13 July 2011.

42 Article 7 (c) of the Data Protection Directive.

43 For instance, it is mandatory to respond to certain requests for information from the Commission (those made on the basis of Article 18(3) of Regulation 1/2003) or the German Cartel Office (Article 59 of the GWB).

44 See WP 117 (supra. fn. 32), in which the Working Party discusses the US Sarbanes-Oxley Act (SOX) which was adopted by the US Congress in 2002, and finds that SOX whistleblowing provisions may not be considered as a legitimate basis for processing on the basis of Article 7 (c) of the Data Protection Directive.

45 Article 2 (f) of the Data Protection Directive, which is not applicable to the processing of sensitive data (to which a more limited set of legal grounds applies). Reliance on the legitimate interest criterion may become more difficult in the future, if proposals to make the application of this criterion subject to additional criteria (see the Draft Report (PE 501.927v04-00) on the proposal for a regulation by Jan Philipp Albrecht, the rapporteur to the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs, EP 2012/0011(COD) 16 January 2013, available at:

of the legitimate interests pursued by the controller (or by the third party or parties to whom the personal data is disclosed), except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

This criterion requires that a balance be struck between the controller's or third party's interest in processing the personal data and the interests of the data subjects concerned not to have their personal data processed. Such balancing cannot be carried out in the abstract, but only on a case-by-case basis taking into account factors, such as proportionality, the seriousness of the alleged offences (e.g., criminal offences vs. violation of company policies) and the consequences for the data subjects (e.g., disciplinary action or criminal or administrative sanctions),[46] including the degree of intrusion (e.g., random checks vs. continued monitoring) and safeguards put in place.

It would be a mistake to consider that the company's interests (for instance, to defend itself in competition law proceedings or to prevent anti-competitive behaviour) will always outweigh the employees' interests, especially where individual employees may face severe consequences as a result. The right to data protection is a fundamental right and, as such, bears great weight.[47] As the Working Party has stated, employees do not abandon their right to privacy and data protection at the door of their workplace. It would also be irrelevant whether the personal data in question has been generated during working hours or by using the employer's equipment.[48] Employees would have a

---

http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE501.927) are successful.

[46] For instance, in certain EU Member States, such as Germany, individuals may also face sanctions as a result of a violation of competition law.

[47] The Charter of Fundamental Rights of the European Union (the "Charter"), OJ C 364, 18.12.2000, pp. 1–22 (Articles 7 and 8) and the TFEU (Article 16) have elevated data protection to a fundamental right at EU level. Even if the right to data protection contained in the Charter and the TFEU does not directly create obligations of private parties, the EU member states' obligations thereunder arguably involve the adoption of measures designed to secure respect for data protection by private parties in their relation with other individuals. The Data Protection Directive can possibly be considered as an expression of such 'horizontal obligations'. See Juliane Kokott and Christoph Sobotta, "The Distinction between Privacy and Data Protection", *International Data Privacy Law*, September 15, 2013.

[48] Contrast this with Cour de Cassation (Soc.), decision No. 12-12138 of 15 August 2013, *Mr. X v. Company Y&R*, available at www.legifrance.gouv.fr, in which the French Supreme Court held that folders and files created by an employee using the IT that his employer put at his disposal for the performance of his job duties are presumed to be professional and may be accessed by the employer in the employee's absence, unless the employee identifies them as being private. E-mails and files that are stored on the professional hard disk of the employee should not automatically be considered private merely because they originate from the employees' personal mailbox. That said, access to the employee's personal files or e-mails sent from the employee's personal e-mail address in the absence of the employee was considered to violate the employees' right to privacy.

legitimate expectation of a certain degree of privacy in the workplace, even if the companies' use or IT policies often state the contrary.

In sum, the above discussion makes it clear that employers cannot take it for granted that they have an unlimited right to search through their employees' e-mail accounts, computer or paper files as they wish. They carefully need to determine the legal basis for any data processing activities in the context of investigations on a case-by-case basis.

B. Data Quality

Any data processing must comply with what is often referred to as the "data quality" principle:[49] the personal data collected and processed should be adequate, relevant and not excessive; only the minimum necessary data should be processed; personal data must not be kept for longer than necessary; and personal data must be accurate and, where necessary, kept up to date. The data quality principle is also closely linked to the "purpose limitation" principle, pursuant to which personal data must be collected for a specific purpose and may not be further processed for incompatible purposes.[50]

The DG Competition's Privacy Statement essentially repeats the applicable principles, without providing much detail as to the way in which the Commission intends to apply them in practice :

> "The various competition regulations also guarantee that any data is collected for specified, explicit and legitimate purposes. The data may only be collected and further processed for the purpose of applying the EC competition rules and in respect of the subject matter for which it was collected.
>
> There are also sufficient guarantees that data are adequate, relevant and not excessive in relation to the purposes for which they are collected. This proportionality test is reflected in various provisions of the different competition regulations."

The data quality principle has several implications for competition law investigations. First, the purpose and scope of an investigation must be clearly defined in an investigation mandate and plan, setting out the investigation's purpose, keywords for searches and instructions on how to handle personal data. In other words, the data quality

---

[49] Article 6 of the Data Protection Directive and Article 4 of the Regulation.

[50] Working Party Opinion 03/2013 on purpose limitation (WP 203), adopted on 2 April 2013.

principle is incompatible with fishing expeditions. The investigation needs to be narrowly focused, limiting the records to be looked at to the subject-matter of the investigation, the relevant time period and the relevant individuals in the relevant departments.[51] Private e-mails and documents need to be filtered out and separated from work-related documents. This means that rather than copying entire inboxes or hard disks or all folders from employees' drives, competition law officials should use keywords or algorithmic searches to collect only documents that are relevant to the investigation in question.

Moreover, only the minimum data necessary should be processed, the least intrusive methods used (e.g., screening of anonymised/aggregated/high-level data instead of individualised data, automated scanning rather than review in person) and, where possible, screening results, protocols and notes should be anonymised or at least pseudonymised. Similar considerations should be applied in case of disclosure of personal data to third parties, including cartel victims and law enforcement authorities. Finally, appropriate retention periods[52] need to be defined and after the expiry of the maximum retention period personal data has to be redacted, anonymised or deleted.

These requirements are to a certain degree reflected in the good practices promoted by the ICN's Anti-Cartel Enforcement Manual[53] and the recently revised DG Competition's practice of digital evidence gathering:[54]

> Dawn raids are carried out on the basis of the inspection decision (mandate), which defines the scope of the investigation. Once at the business premises, DG Competition starts by locating the target devices and extracting possible relevant files, which will be uploaded on a mobile server on the company

---

[51] By contrast, in *Deutsche Bahn AG and Others v European Commission* (supra fn. 3) the General Court supported the Commission's broad powers of inspection and to search exhaustively offices and documents, even if there is no clear indication that they contain information related to the investigation.

[52] In WP 117 (supra fn. 32), the Working Party suggested that personal data processed by a whistleblowing scheme should be deleted, promptly, and usually within two months of completion of the investigation of the facts alleged in the report. When legal proceedings or disciplinary measures are initiated against the incriminated person or the whistleblower in cases of false or slanderous declaration, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal. Personal data relating to alerts found to be unsubstantiated by the entity in charge of processing should be deleted without delay.

[53] See, for instance, section 8.1.: "[…] *to be cautious in drafting the scope and wording of terms in search warrants or record production orders.*"

[54] For a detailed description of the Forensic IT procedure and workflow used by the Commission's Forensic IT group, see Nathalie Jalabert-Doury, Dirk Van Erps, "Digital evidence gathering: An update", *Concurrences* N° 2-2013, art. No 52013, pp. 213-219.

> premises and reviewed by Commission officials for relevance ("[b]*y looking at the header of the document and/or the rough content, an officer can generally determine whether a document is legally privileged or private*"). Commission officials will tag any relevant documents and only these will subsequently be copied on a data carrier for the officials to take with them to Brussels. It is also understood that – similar to the procedure applied in case of legally privileged documents – a company representative could point out which documents are likely to be private and the inspectors will judge the validity of the claim in a *prima facie* assessment. If approved, these documents are removed from the device to be copied. In case of disagreement, a formal protest can be made and the sealed envelope or 'continued inspection' procedure would apply.[55]

Pursuant to the Privacy Statement issued by DG Competition on its website, "[t]*he various competition regulations ensure that data are accurate and where necessary kept up to date, since they provide the Commission with various instruments (e.g., written requests for information) to check with the relevant sources whether the data are indeed accurate*" and competition files are conserved until closure of the case following which the paper file is archived.

Whilst this procedure puts certain safeguards in place which could help complying with the data quality principle, there are some loopholes. First, as DG Competition does not normally provide a list of keywords to the companies that are inspected, it is difficult for them to verify whether the keywords have been properly selected so as to exclude the gathering of irrelevant documents.[56] The relevance of documents is defined by the Commission officials looking at the individual documents and Commission officials are free to choose the search terms. Second, DG Competition explicitly reserves the right to make a forensic image of an entire hard disk or inbox as "*the content of the documents cannot always be studied or looked into at the business premises*".[57] This implies that,

---

[55] If a dispute arises between the inspectors and the company as to the content of a specific document and whether the inspectors can look at it and make a copy of it, the official may place a copy of the contested document in a sealed envelope and then remove it and bring it to DG Competition's premises, with a view to a subsequent resolution of the dispute. See Commission notice on best practices for the conduct of proceedings concerning Articles 101 and 102 TFEU, OJ 2011 C 308/6, 20 October 2011, para. 54.

[56] By contrast, the German Federal Cartel Office discloses the used search terms. See Saller, supra fn. 35.

[57] Ibid, fn. 54.

contrary to the principle of data minimisation, all data on the target device is copied.[58] This increases the likelihood that large amounts of irrelevant records are being copied and reviewed outside the legitimate scope of the investigation mandate. Third, the Commission does not typically redact personal data from seized documents or anonymise or delete personal data unless it is requested (by the parties) to do so.[59] Finally, DG Competition and national competition authorities may in certain instances invoke an exemption or restriction to the application of the data quality principle.[60]

In this respect, the approaches followed by national competition authorities vary across the EU. We have seen, for instance, that the French Supreme Court upheld the inspectors' position that they cannot "split" electronic mailboxes to seize only the relevant emails without materially altering the reliability of the information extracted.[61] By way of contrast, the Dutch competition authority uses keywords to identify and separate digital data that is within the scope of the investigation from "possibly out-of-scope" data. Further screening is then performed at the Dutch authority's premises by its IT specialists – who are not involved in the substantive aspects of the investigation – and irrelevant or protected data is returned to the company.

The problem that competition authorities may come across private and other materials unrelated to the investigation has also been discussed at the ICN's annual conference in April 2013 where participants reportedly raised concerns that authorities "cast too wide a net when searching the entire contents of computers looking for evidence."[62] The problem of potential access to private data will be exacerbated with the increasing

---

[58] For similar practices ("[t]*he data carrier on which the digital information is stored will often be copied and further examined at the* […] *agency.*") see also ICN Anti-Cartel Enforcement Manual, Digital Evidence Gathering, section 8.3.

[59] The Commission would however, in principle, remove personal data from documents before their publication. See DG Competition's Antitrust Manual of Procedures (supra fn. 30), Publication of Decisions, Chapter 28, paras. 56 and 102.

[60] Pursuant to Article 20 of the Regulation, EU institutions may restrict the application of several Articles of the Regulation, including Article 4 (1) (Data quality), where such restriction constitutes a necessary measure to safeguard, for instance, (b) an important economic or financial interest of the European Union or (e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (b). In such a case the data subject shall be informed. Similarly, Article 13 of the Data Protection Directive.

[61] See above discussion in Section II, 1st para. See also, e.g., Cour de cassation (Crim.), 11 January 2012, No 10-87.087, available at www.legifrance.gouv.fr. For a detailed discussion of the relevant French case law and potential evolution, see Nathalie Jalabert-Doury, "Les saisies informatiques en France après l'évolution de la méthodologie de la Commission : enfin un peu de lumière au bout du tunnel ?", *Concurrences* N° 2-2013, art. No 52013, pp. 213-219.

[62] Ron Knox, "Privacy worries arise when enforcers grab hard drives", *Global Competition Review*, 25 April 2013.

popularity of "Bring Your Own Device" (also referred to as BYOD) policies, as employees' own personal devices will by definition contain private data.[63] BYOD also raises the question of the extent to which competition authorities may access employee owned devices.

There is also no guarantee that provisionally or otherwise copied data is not used for other purposes than initially foreseen. This risk has again been illustrated in the *Deutsche Bahn* ruling in which the General Court confirmed that the Commission was not prevented from using evidence incidentally gathered in one investigation for another investigation. However, as a matter of principle, evidence obtained without legal justification should not be used, whether as direct evidence or incidentally as a source of or lead to evidence.[64]

Companies have to respect the data quality principles and should provide clear guidance to their audit and compliance teams and other employees involved in investigations. For instance, the guidance should set out the steps to follow so as to avoid the gathering or accessing of private data (e.g., by using tailored key words, filtering, anonymisation or redaction, documentation) and how to deal with personal and private data (e.g., instruction to immediately destroy or delete private data). Companies should also define retention periods for data and ensure compliance with the data retention schedules.

C. Information to be Given to Data Subjects

Companies may often want to carry out investigations in secret, with little or no publicity. However, covert investigations (as possibly mock dawn raids) may run counter the principle of transparency, which is one of the cornerstones of EU data protection law.

Under the Data Protection Directive, the controller must inform data subjects about the identity of the controller, the purposes of the processing and any further information, such as the recipients of the personal data and the existence of the right of access and rectification, in order to guarantee fair processing.[65] Individuals must not only be

---

[63] BYOD refers to companies' practice or policy of allowing employees to use their personally owned mobile devices instead of company owned devices to access and sometimes even store company information and applications. BYOD raises a number of challenges, including from a data protection perspective, which should be addressed from the outset, such as ensuring a clear separation between business and private data (for instance, by using sandbox technology).

[64] See Temple Lang, supra fn. 4.

[65] Article 10 of the Data Protection Directive.

informed if data is collected directly from them, but also if the data is collected from a third party.[66] Similar (even slightly broader) information obligations apply under the Regulation.[67]

The Privacy Statement, published on the Commission's website, provides most of the required information, including the purpose of the data collection, the recipients of the data and the existence of the right of access and information. However, the information about the categories of data collected is obviously incomplete or misleading (as the Privacy Statement presently limits the data to the names, contact details and the position of the natural person in the undertaking). Obviously, information collected during an inspection may contain all kinds of other personal data, including not only that of data subjects in the undertaking itself, but also of others (including correspondents and employees of customers, suppliers, competitors, etc.). From the Commission's Explanatory note to an authorisation to conduct an inspection it even appears that the Commission tries to partly delegate its information obligation to the companies.[68]

EU institutions and bodies, as well as national public authorities may also restrict the application of the information obligation, for instance, where this is necessary to safeguard an inspection.[69] However, under the Regulation, in this case the data subject shall be informed of the principal reasons on which the restriction is based and of his or her right to have recourse to the EDPS. It is not clear whether DG Competition relies on this exception and, if so, how it complies with this information obligation as the Privacy Statement is silent on this issue.

The Data Protection Directive also provides for exceptions to the information obligation on which companies may rely, for instance, when the application of this obligation proves impossible or would involve a disproportionate effort.[70] Companies should not, however, too easily rely on one of these exceptions. This is because they have been implemented in different ways at national level and many supervisory authorities are

---

66 Article 11 of the Data Protection Directive.

67 Articles 11 and 12 of the Regulation. For instance, the Regulation expressly mentions the legal basis of the processing operation and the time-limits for storing the data as possible examples of further information which may need to be provided to data subjects.

68 Supra fn. 7 at para. 11: "*When such actions* [e.g., the temporary blocking of individual email accounts, removing and re-installing hard drives from computers and providing 'administrator access rights'-support] *are taken,* […] *it is* *the undertaking's responsibility to inform the employees affected accordingly*." (emphasis added)

69 Article 20 of the Regulation and Article 13 of the Data Protection Directive.

70 Article 11 (2) of the Data Protection Directive. Similarly, Article 11 (2) of the Regulation.

reluctant to accept reliance on them in the case of corporate investigations. Some Member States' laws provide for an exemption to the information obligation when providing notice could jeopardise the proper conduct of the investigation[71] or the gathering of the evidence, lead to a destruction of evidence or prejudice the detection or prosecution of a criminal offence. However, there usually needs to be a credible risk and the exception should be applied restrictively on a case-by-case basis. Moreover, the information obligation is usually suspended only for the time these risks exist.

Companies are therefore well advised to address data processing in the context of investigations in their general policies and information notices. Although this may not exempt them from the obligation to provide specific notice in a particular case, this together with the existence of information notice templates and clear instructions as to when and how to provide notice will greatly facilitate compliance with the transparency requirement.[72]

D. Rights of Data Subjects

Controllers are responsible for ensuring that data subjects can exercise their rights to request access to their personal data, obtain the rectification, erasure or blocking of personal data where such data is incomplete or inaccurate or where the processing of such data is unlawful, and object to the processing of their personal data in particular if the processing is based on the "legitimate interest" criterion as a legal basis, provided there are compelling grounds relating to the person's particular situation.[73]

Exceptions designed to protect the investigative process exist in some EU Member States. However, even in those instances, the exception would only allow for a temporary suspension of the data subjects' rights. DG Competition and the national competition authorities may also rely on exceptions and restrictions of the scope of the data subjects' rights,[74] and DG Competition apparently invokes this exception in a sweeping manner:[75]

> "Natural persons who are not the addressees of a Statement of Objections have no such rights. Granting them right of access, blocking and erasing of

---

[71] See also WP 117 (supra fn. 32).

[72] For instance, in the context of pre-trial discovery, the Working Party has suggested that, in addition to an advance, general notice of the possibility of personal data being processed for litigation, on-time notice should be given where the personal data is actually processed for litigation purposes. See WP 158 (supra fn. 32).

[73] Articles 12, 14 and 15 of the Data Protection Directive and Articles 13-19 of the Regulation.

[74] Article 20 of the Regulation and Article 13 of the Data Protection Regulation.

[75] See Privacy Statement, supra fn. 26.

> data would hinder the monitoring and inspection tasks of the Commission when enforcing competition law, which is necessary to safeguard important economic or financial interests of the European Communities (i.e. the proper functioning of competitive markets). The exceptions of Article 20(1) sub b) and sub e) of Regulation 45/2001 therefore apply in these cases. However the data subject will have the chance to address the mailbox mentioned in the privacy statement a request of the deletion or modification of his/her data which had allegedly been unlawfully processed." (emphasis added)

This interpretation does not seem to be in line with statements of the EDPS, according to which restrictions to a fundamental right cannot be applied systematically. Instead, a case-by-case assessment of the circumstances of the data processing in question is required.[76] Moreover, it is questionable how data subjects can request the deletion or modification of their data without first obtaining access. Data subjects are thus in practice deprived from exercising their rights at least vis-à-vis the Commission. Even if there may be good reasons to invoke exceptions prior to the issuance of a Statement of Objections, it is difficult to see how the invocation of such exceptions can remain justified during all stages of an investigation and thereafter.

Companies should have in place appropriate procedures so as to ensure that data subjects can exercise their rights effectively at all stages of an investigation and thereafter and rely on exceptions with caution.

---

[76] See, for example, the Opinion on a notification for Prior Checking received from the Data Protection Officer of the European External Action Service on security investigations of the EDPS of 1 February 2013 (2011-1059) which states: "[…] *if the EEAS uses an exception to defer the provision of information, it should take into account that the restrictions to a fundamental right cannot be applied systematically. The EEAS must assess in each case whether the conditions for the application of one of the exceptions of Article 20.1.a or Article 20.1.c may apply. In addition, as foreseen in Article 20 of the Regulation, the measure has to be "necessary". This requires that the "necessity test" has to be conducted on a case-by-case basis. If the EEAS uses an exception, it must comply with Article 20.3 according to which "the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor". However, the EEAS may avail itself of Article 20.5 to defer the provision of this information as set forth in this Article: "Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect". In the light of this, and contrary to what is stated in the EEAS notification, only temporary deferrals are allowed. The EEAS cannot definitely "refuse" the access to the data.* […]."

E. Confidentiality and Security of the Processing

Both the Directive and the Regulation contain rules on confidentiality and security of the processing so as to protect personal data. Moreover, employees with access to personal data must in principle not process them except on instructions from the controller.[77]

Commission officials are subject to a professional duty of secrecy, whereas companies have to contractually impose confidentiality obligations on their employees (which is even mandatory in Germany, for example).

As regards data security, controllers must implement appropriate technical and organisational measures to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and all other unlawful forms of processing.[78] For instance, personal data should not be sent by e-mail over the Internet, but either be encrypted or sent via a secure Internet connection or placed in secure repository or data room, preferably in the country of origin. Companies' security policies will usually cover the processing of personal data in the course of investigations. It may nonetheless be advisable to recall some of the most pertinent rules in the investigations manual and to set out typical steps to take in this respect. For instance, before submitting documents to a competition authority, the organisation should filter the documents or make an express claim for confidential treatment of personal data and provide a non-confidential version of documents with personal data being redacted.

Security measures applied by the Commission in the context of an inspection include, for instance, encryption of data carriers and sanitising all Commission equipment that has been used to store digital information of the company before leaving the company.[79] The ICN's Anti-Cartel Enforcement Manual recommends the use of tools that are thoroughly tested and generally accepted in the computer forensics field.

Ensuring data protection awareness and training of staff members is relevant both for companies and competition authorities. The ICN's Anti-Cartel Enforcement Manual acknowledges that it is good practice for competition authorities to have a dedicated internal organisation or staff capacity to undertake digital evidence gathering and to give special training to the agency's staff that collect and process digital evidence.[80]

---

[77] Article 16 of the Data Protection Directive and Article 21 of the Regulation.

[78] Article 17 of the Data Protection Directive and Article 22 of the Regulation (which also sets out different security objectives).

[79] Supra fn. 54.

[80] Supra fn. 27.

F. Registration

At national level, data processing might be subject to prior notification, prior checking and/or prior authorisation by the national data protection authorities (together referred to as "registration").[81] The evaluation of whether a particular processing operation falls under any registration requirements depends on the national legislation and the practice of the national data protection authority, which differ significantly among Member States. The registration process may sometimes take considerable time (even up to several months), which often conflicts with the requirement to act quickly. Companies that have covered data processing in the context of investigations in their existing registrations with national data protection authorities may gain precious time.

At Commission level, the registration process has been internalised: any processing operation only needs to be notified to the data protection officer (which each EU institution and body shall appoint) who keeps a register of notified processing operations (similar to the register kept by national data protection authorities).[82] Processing operations likely to present specific risks are subject to so-called prior checking by the EDPS,[83] but so far the EDPS has not published any opinion dealing with data processing by DG Competition in the context of competition investigations.

G. International Data Transfers

In some instances, companies are required to produce documents and other relevant elements of information in relation to competition law investigations or litigation taking place outside the EEA. The supervisory authorities generally take the view that remote

---

[81] Articles 18 to 20 of the Data Protection Directive.

[82] Articles 25-25 of the Regulation and Article 21 of the Data Protection Directive. Under the proposed GDP Regulation the registration requirements would essentially be abolished and instead companies required to keep their own register of processing operations (similar to the current situation under German data protection law).

[83] Article 27 of the Regulation (see also the proposed GDP Regulation). The EDPS describes prior checks as follows: Prior checks serve to determine whether the EU administration is planning to process personal data in compliance with the Regulation, or whether the system needs to be improved from a data protection point of view. In principle, the opinion of the EDPS is to be delivered prior to the start of the processing operation. The findings of the EDPS take the form of a prior check opinion which is presented to the controller and to the data protection officer of the institution or body concerned. The opinions usually imply that the institution or body needs to adopt a set of recommendations.

accessing and viewing of personal data retained in the EEA from outside the EEA amounts to a transfer of personal data.[84]

Both the Directive and the Regulation start from the basic premise that personal data may only be transferred to a third country if an adequate level of protection is ensured in that country.[85] "*Adequacy*" is assessed on a case-by-case basis "*in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations*."[86] So far, only a small number of countries, namely Andorra, Argentina, Canada, the Faeroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay, have been recognised as providing an adequate level of protection by the Commission.[87] In contrast with these "white listed" countries, the level of protection in the US,[88] China or India, for example, is not considered to be adequate.

If the importing country is not "white-listed", the controller must provide adequate safeguards with respect to the protection of the privacy and fundamental rights of the individuals, for instance, by concluding a data transfer agreement with the non-EU data recipient.[89] The Commission has adopted three sets of standard contractual clauses which controllers can use in this respect. Although this is less common, controllers can also prepare their own contracts.[90] Binding Corporate Rules ("BCRs") are another transfer

---

[84] In contrast with this, in its judgment in Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, para. 71, the Court held that "*there is no 'transfer* [of data] *to a third country' within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.*"

[85] Article 25 of the Data Protection Directive and Article 9 of the Regulation.

[86] Article 25 (2) of the Data Protection Directive.

[87] See at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[88] However, personal data may be transferred to US organisations which have self-certified under the US Safe Harbour scheme (see Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25 August 2000, p. 7). See also at: http://export.gov/safeharbor/.

[89] Article 26 (4) of the Data Protection Directive and Article 9 (7) of the Regulation.

[90] Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, OJ L181/19, 4 July 2001; Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L385/74, 29 December 2004) and Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L39/5, 12 February 2010, which has repealed an earlier decision, Decision 2002/16/EC.

mechanism on which companies may rely.[91] However, BCRs are internal rules defining a multinational group's global policy with regard to the international transfer of personal data and as such only apply to intra-group data transfers. In other words, BCRs do not cover transfers to a company which does not belong to that group, such as lawyers, a court or public authorities.

Companies are well advised to consider available transfer solutions in advance. Only when relying on such safeguards is not practical and/or feasible, the controller may rely on one of the statutory derogations listed in the Data Protection Directive (or the Regulation).[92] The statutory derogations that are typically considered in the context of competition law or corporate investigations are consent, important public interest and establishment, exercise or defence of legal claims, but all of them have their limitations.

1. Consent

Data transfers may be based on the data subject's unambiguous consent.[93] However, for the same reasons as discussed in section V.A.1. above, consent should be used with caution and often provides a false good solution.

2. Important Public Interest

Data transfers may also be permitted where they are necessary or legally required on important public interest grounds.[94] The Working Party interprets this statutory derogation narrowly and only recognises important public interests identified by the national legislation applicable to controllers established in the EU, but not where the transfer is of interest only to one or more public authorities in a third country. It would "*not* [be] *acceptable for a unilateral decision by a third country, on public interest grounds specific to it, to lead to regular bulk transfers of data protected by the*

---

[91] The Data Protection Directive does not contain provisions concerning the use of BCRs, but the Working Party has set out the framework for the structure of such BCRs and the necessary elements to be included in them in several opinions. Since 1 January 2013, BCRs have also become available for processors. The proposed GDP Regulation also explicitly recognises BCRs.

[92] Article 26 (1) of the Data Protection Directive and Article 9 (6) of the Regulation. In the Working Party's view, the derogations shall only be used where transfers are neither recurrent, nor massive or structural. See Working Document 12/1998: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP 12), adopted on 24 July 1998.

[93] Article 26 (1) of the Data Protection Directive and Article 9 (6) (a) of the Regulation.

[94] Article 26 (1) (d) of the Data Protection Directive and Article 9 (6) (d) of the Regulation.

Directive".[95] In comparison, the "public interest" derogation may provide a legal basis for data transfers between competition authorities.[96]

3. Establishment, Exercise or Defence of Legal Claims

The statutory derogation most commonly relied upon by private companies in the context of investigations allows data transfers that are necessary for the establishment, exercise or defence of a legal claim.[97] However, remote and speculative prospect claims will usually not suffice; claims must rather be extant or imminent. Moreover, the provision will only justify single, unique or limited data transfers.[98]

The Working Party considers that responses to third country law enforcement authorities' or courts' requests for materials containing personal data are particularly problematic. It requires that the international rules governing criminal or civil proceedings be complied with, notably as they derive from the provisions of the Hague Conventions of 18 March 1970 (the "Taking of Evidence" Convention)[99] and of 25 October 1980 (the "Access to Justice" Convention).[100] The Working Party specifically recognises that compliance with a request made under the Hague Convention would provide a formal basis for a transfer of personal data.[101] However, not all Member States have signed the Hague Convention and some Member States have only signed with reservations, which makes it in some cases extremely difficult if not impossible for companies to transfer documents to third parties abroad (for instance, in response to document requests).[102]

---

[95] Working Party Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114), adopted on 25 November 2005.

[96] As has been acknowledged in recital 87 of the proposed GDP Regulation.

[97] Article 26 (1) (d) of the Data Protection Directive and Article 9 (6) (d) of the Regulation.

[98] WP 12, supra fn. 92.

[99] Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, available at: http://www.hcch.net/index_en.php?act=conventions.text&cid=82.

[100] Convention of 25 October 1980 on International Access to Justice, available at: http://www.hcch.net/index_en.php?act=conventions.text&cid=91. Similarly, although within the EU, the question to what extent a UK court may order a plaintiff in a UK damages action to disclose corporate data held in France is reportedly the subject of proceedings before the UK Court of Appeals, see "Areva, Alstom say disclosing cartel data in damage claim breaches France's sovereignty", *MLex*, 25 June 2013.

[101] Working Document 1/2009 on pre-trial discovery for cross border civil litigation (WP 158), adopted on 11 February 2009.

[102] For instance, the French blocking statute No. 68-678 of 26 July 1968 (*Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères*) prohibits the transfer of any information in view of establishing evidence in any non-French proceedings. For best

4. Bilateral International Agreements

The Commission or national competition authorities may also be able to rely on bilateral international agreements as a legal basis for international transfers of personal data. The EU has entered into antitrust cooperation agreements with the US (1998), Canada (1999), Japan (2003) and South Korea (2009).[103]

To date, international antitrust data sharing has remained limited in that the respective competition authorities may share "confidential information" only if they have obtained a waiver from the companies/persons that have provided such information.[104] In other words, the company concerned by the investigation must give its green light to the sharing of its information. The existing bilateral agreements do not elaborate on the treatment of personal data specifically. This may, however, change with the next "generation" of competition cooperation agreements. For instance, the EU and Switzerland (a white-listed country) recently signed a cooperation agreement,[105] which allows the respective competition authorities to share confidential information without the need to obtain waivers, subject to certain safeguards.[106] Notably, the competition authority that receives confidential information may use it only to investigate the same or related conduct.[107] The EU-Switzerland agreement is also different in that it requires the

---

practices, recommendations and principles for addressing the preservation discovery of protected data in U.S. litigation, see also the project of *The Sedona Conference International Principles on Discovery, Disclosure & Data Protection*, available at: https://thesedonaconference.org/.

[103] Agreement between the European Communities and the Government of the United States of America on the application of positive comity principles in the enforcement of their competition laws, OJ L 173, 18 June 1998; Agreement between the European Communities and the Government of Canada regarding the application of their competition laws, OJ L 175, 10 July 1999; Agreement between the European Community and the Government of Japan concerning cooperation on anti-competitive activities, OJ L 183, 22 July 2003; Agreement between the European Community and the Government of the Republic of Korea concerning cooperation on anti-competitive activities, OJ L 202, 4 August 2009. These agreements are also available on DG Competition's website at: http://ec.europa.eu/competition/international/bilateral/index.html

[104] See, for example, article IV.2 of the EU-US agreement, article VII of the EU-Canada agreement, article 4.4 of the EU-Japan agreement, article 4.4 of the EU-South Korea agreement.

[105] Agreement between the European Union and the Swiss Confederation concerning cooperation on the application of their competition laws. The agreement still needs to be ratified by the European and Swiss Parliaments. The draft agreement can be found in the Proposal for a Council Decision on the conclusion of an Agreement between the European Union and the Swiss Confederation concerning cooperation on the application of their competition laws, COM(2012) 245 final (the "Proposed EU-Switzerland Agreement"). For additional information, see Commission press release, "European Union and Switzerland sign Cooperation Agreement in Competition Matters", 17 May 2013 (IP/13/444).

[106] Proposed EU-Switzerland Agreement, recital 4 and article VII(4).

[107] Proposed EU-Switzerland Agreement, articles VII(4) and VIII.

parties to protect personal data in accordance with their respective legal regimes when they cooperate.[108] The EU-Switzerland agreement is thus a sign of increased awareness of data protection-related aspects relating to competition investigations. According to press reports, the Commission may propose, in the framework of the ongoing negotiations of the Transatlantic Trade and Investment Partnership ("TTIP"), a similar provision that would facilitate the exchange with the US of confidential information on mergers and other investigations without the companies' permission.[109]

DG Competition will seek access to all relevant electronic information regardless of the physical location of the servers on which it is stored or the storage in the cloud.[110] This extra-territorial reach of DG Competition's and national competition authorities' investigation powers may conflict with the rules applicable in third countries from where they retrieve the relevant data.[111] Companies such as SWIFT have come under the scrutiny of both the Working Party and national data protection authorities for having given foreign law enforcement authorities access to personal data kept in the EU.[112] By accessing information kept outside the EU, DG Competition and national competition authorities may put foreign companies in a similarly difficult situation under their respective national laws.

---

[108] Proposed EU-Switzerland Agreement, article IX(3), and recital 10, in which the Commission restates its position that the Swiss data protection rules can be considered equivalent to the EU rules. The Commission indeed recognised in a previous decision that Switzerland provides an adequate level of protection for personal data transferred from the EU; see Commission Decision of 26 July 2000 on the adequate protection of personal data provided in Switzerland, OJ L 215, 25 August 2000, p. 1.

[109] Notwithstanding the fact that data protection issues have generally been cut out of the negotiations for the TTIP. See Jeremy Fleming, *TTIP: Data is the elephant in the room*, Special Report, published 24 September 2013, EurActiv, available at http://www.euractiv.com.

[110] Supra fn. 54 and for Germany see Saller, supra fn. 35. The Working Party defines cloud computing as a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. See Opinion 05/2012 on Cloud Computing (WP 196), adopted on 1 July 2012.

[111] Aitor Ortiz, "Clouds behind the Clouds", *World Competition* 36, no. 1 (2013), pp. 61-84, who also makes the interesting argument that cloud computing may facilitate cartels and prevent antitrust authorities from finding evidence of the cartel conduct.

[112] See, for instance, the Working Party's Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP 128), adopted on 22 November 2006, criticising SWIFT for having provided to a US law enforcement authority personal data, collected and processed via the SWIFT network for international money transfers, on the basis of subpoenas under American law for terrorism investigation purposes.

VI. Consequences of Non-compliance with Data Protection Law

In case of non-compliance with data protection law, data subjects can complain to the competent national supervisory authority. They also have the right to a judicial remedy for a violation of their rights and may claim compensation.[113] Data controllers moreover run the risk of investigations and enforcement actions by the competent supervisory authority. Some supervisory authorities have adopted a "name and shame" policy and inform the public of investigations or enforcement action taken against individual companies. This can significantly damage a company's reputation and brand, as well as its relationship with customers, employees and other data subjects.

Under the Regulation, a data subject may lodge a complaint with the EDPS. If a complaint is admissible, the EDPS usually carries out an inquiry. In most cases, the EDPS will issue a set of recommendations that the controller needs to implement to ensure compliance with data protection rules. The data subject may also bring an action before the General Court.[114] Data subjects also have the right to claim compensation for damages suffered on the basis of Article 340 TFEU.[115]

A major difference between the public (at least at EU level) and the private sector regarding the consequences of non-compliance with data protection rules concerns the possibility of sanctions. The Regulation does not foresee any monetary or other forms of penalties (except for the possibility to take disciplinary action against individual officials or servants in accordance with the Staff Regulations).[116] Conversely, in most EU Member States, the violation of (certain) data protection rules – at least by companies or individuals – is punishable with monetary penalties[117] and, in the most serious cases, with criminal sanctions, including imprisonment. For instance, in 2009, Deutsche Bahn, which had monitored communications and bank details of over 200,000 employees in a corruption investigation, was fined €1.1 million for a violation of data protection rules. In 2008, the former security manager of Deutsche Telekom was sentenced to three and a half years imprisonment for having violated privacy rules when monitoring phone calls of

---

[113] Articles 28 (4), 22 and 23 of the Data Protection Directive.

[114] Article 32 of the Regulation.

[115] Article 340 TFEU states that "[i]*n the case of non-contractual liability, the Union shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its institutions or by its servants in the performance of their duties*."

[116] Article 49 of the Regulation.

[117] For instance, in Germany, the maximum administrative fine is in principle € 300,000, but in certain cases a criminal fine or imprisonment can be imposed, whereas in the UK, the Information Commissioner's Office (the "ICO"), can issue penalties of up to GBP 500,000.

managers, board members and journalists to investigate information leaks to the press. In 2012/13 the UK ICO issued penalties of just over £2.6 million and initiated six criminal cases for serious breaches of the UK data protection law.[118] If the proposed Regulation is adopted, sanctions for data protection violations would become more severe as the proposal includes fines expressed as a percentage of global turnover similar to the fines for an infringement of EU competition law.[119]

Another difference is probably the likelihood of judicial action. Companies are more likely to face legal action (as compared to the Commission or national authorities) when they violate data protection rules in the context of internal investigations, as employees and other data subjects will be concerned that the investigation findings may be used against them. Although data subjects may also bring the Commission or national competition authorities to court, in practice they will be less likely to do so as they are not directly targeted by the Commission's investigation and may not even be aware that their personal data has been processed. The enforcement mechanism therefore imposes more constraints on companies than on the Commission or national competition authorities (except potentially in those countries where individuals also face sanctions for competition law violations). This imbalance is problematic in that it puts the effectiveness of the data protection rules in question. This shortcoming could be remedied if companies could challenge the Commission's or national competition authorities' actions in the course of inspections on the basis of a violation of the applicable data protection rules. However, recent case-law of the General Court seems to protect the Commission's investigation powers, much to the detriment of the rules on data protection:[120]

- First, steps and actions taken by the Commission in the course of inspections may not be directly challengeable before the Court. For instance, the General Court indicated that the Commission's decision during an inspection to copy the content of certain computer files in their entirety and to interview an employee "*are not to be regarded as acts separable from the decision under which the inspection was ordered but as measures implementing that decision*".[121] It follows that, in order

---

[118] See at: http://www.ico.org.uk and the ICO's annual report 2012/13.

[119] The proposed GDP Regulation essentially envisages monetary administrative sanctions, ranging from up to € 250,000 (or 0.5% of the annual worldwide turnover in case of an enterprise) to up to € 1 million (or 2% of an enterprise's annual global turnover), depending on the seriousness of the infringement.

[120] For a similar discussion of the remedies in case of a violation of the right to privacy, see Temple Lang, supra fn. 4.

[121] Case T-135/09 *Nexans France SAS and Nexans SA v European Commission*, [2012] ECR II (not yet published), judgment of 14 November 2012, paras 120-125.

to challenge these measures on the ground of a violation of the fundamental right of data protection, companies would have to wait until the Commission issues its final decision and then try to challenge the final decision. However, in that case the company could do nothing to prevent the Commission from copying and reviewing large amounts of irrelevant material and using it for other purposes in the first place. Alternatively, companies could refuse access to the documents – thus obstructing the inspection – and then challenge the Commission decision taken on the basis of Article 23(1)(c) and (d) of Regulation 1/2003.[122] However, this option not only presumes that the Commission would take such a decision, but also requires the company to expose itself to the risk of substantial procedural fines, even if it can subsequently appeal the fine.

- Second, even in cases where the measures concerned are challengeable acts, the company would need to demonstrate that it has the required legal standing to raise claims relating to the protection of (third parties') personal data. In a case concerning the confidential treatment of information which could prejudice the right to the protection of personal data of employees (allegedly involved in the implementation of the cartel), the General Court indicated that "*the applicant cannot rely on the damage which its employees alone would suffer* […] *rather the applicant must show that such damage is likely to entail – for itself – serious and irreparable harm*".[123] It remains to be seen whether companies will be able to show such harm, despite the high barriers set by the Court.[124]

- The General Court also indicated that companies may bring an action against the Commission for non-contractual liability on the basis of Article 340 TFEU.[125]

---

[122] *Ibid*, paras 126 and 132.

[123] See Case T-462/12 R *Pilkington Group Ltd* v *Commission* [2013] ECR II (not yet published), order of 11 March 2013, para. 40. The Commission's appeal against the order has been dismissed, see Case C-278/13 P(R), [2013] ECR II (not yet published), order of 10 Setpember 2013, available at http://eur-lex.europa.eu.

[124] *Ibid*, para. 41, where the General Court states that "[t]*he applicant thus confines itself to a vague and speculative assertion but does not provide any details in that regard or substantiate its assertion with any evidence. The same is true of the assertion that its employees might bring actions claiming that it has failed to protect them. In particular, it has not maintained, let alone shown, that it would be in the interests of the sound administration of justice for it to ensure the collective defence of the interests of the employees concerned on the ground that they cannot be required, because there are so many of them, to bring separate actions to secure protection of their personal data. Consequently, the applicant has not succeeded in establishing that the alleged damage to the interests of its employees would entail serious and irreparable harm for its undertaking as such.*"

[125] Case T-135/09 *Nexans*, supra fn. 121, para. 133, regarding the Commission decision to take a copy of several computer files and a hard drive and to request information from an employee during the investigation.

However, the question of legal standing to bring such an action may raise similar problems.

- A company may potentially also claim compensation for a breach of privacy under Article 7 of the Charter and ask for interim measures.[126] In this respect it is worthwhile to mention a recent court ruling in the Netherlands. A Dutch court reportedly overturned on the basis of the right to privacy a Euro 3 million fine, which the Dutch competition authority had imposed on executives and companies in the construction market. More specifically, the court criticised the fact that in the proceedings in question a public prosecutor had shared with the competition authority information obtained from wiretaps without sufficient justification - he had not properly weighed the individuals' rights to privacy against the public interest in enforcing competition law.[127]

VII. Conclusion

Following the elevation of data protection to a fundamental human right, the increased sensitivity of individuals concerning their personal data and the forthcoming reform of the European data protection legal framework, data protection law will only gain importance in the future. Both public authorities and companies have to comply with data protection rules. This is an increasingly complex and demanding task not only because of the sheer volume of data stored and processed in different formats (e.g., email, instant messaging, etc.) on different types of devices (e.g., PCs, smartphones, etc.) and in different locations (e.g., servers located across the globe), but also because of the proliferation of various – often inconsistent – data protection legal frameworks globally.

In the absence of specific provisions regarding EU competition law investigations, the general data protection rules must be applied. Although the same data protection principles generally apply to both public authorities and companies, DG Competition and the national competition authorities not only benefit from certain exceptions and restrictions, which are not available to companies, but it is also easier for them to justify the processing and transfer of personal data based on their powers as public authorities. The Commission and the national competition authorities are thus privileged when it comes to data protection compliance. This situation is unlikely to change in the future as the proposed GDP Regulation contains a number of exceptions and restrictions for public

---

[126] See Temple Lang, supra fn. 4.

[127] See "Dutch court overturns antitrust fines in construction sector on privacy grounds", *MLex*, 17 June 2013, and a similar second case, "Dutch court throws out waste-collection cartel over misused wiretaps", *MLex*, 12 July 2013. The Dutch competition authority has appealed both rulings.

authorities and the Council has requested even more flexibility regarding the application of data protection rules in the public sector.

Double standards also apply when it comes to the consequences of non-compliance with data protection rules. DG Competition and national competition authorities usually do not face the same sanctions as companies. In particular, the Commission and most national competition authorities are not subject to monetary sanctions in case of a violation of data protection rules.

Questions regarding the extent to and the conditions under which companies can invoke a violation of data protection rules and the fundamental right to data protection in order to seek annulment of an inspection and/or a final decision will certainly be raised in future cases. The General Court does not seem to have ruled out this possibility entirely,[128] although it currently seems very difficult for companies to show a violation of their own rights (e.g., rights of defence) when data protection rules have been breached. To give effect to the rule of law and the fundamental right to data protection, it could be argued that competition authorities should be prevented from relying on evidence which they have gathered in violation of data protection rules, similarly to the "fruit of the poisonous tree" doctrine in US law.[129] The Dutch court ruling quoted above could be the indication of a new trend whereby courts may be increasingly willing to listen to arguments based on data protection law and in certain circumstances be prepared to annul decisions on the basis of a failure to respect the right to data protection. (However, notwithstanding that it was not based on data protection law considerations, the *Deutsche Bahn* ruling seems to point in the opposite direction.)

The Dutch court approach could have far reaching effects, primarily benefitting companies allegedly involved in anticompetitive behaviour rather than the individuals whose rights are affected by the violation. However, with proper procedures in place, competition authorities could minimise the risk of violating the applicable data protection rules and still gather the evidence required to effectively perform their tasks. In this context, the possibility of evidence being declared inadmissible could be an effective deterrent and help ensuring compliance with applicable data protection rules even by public authorities, thus giving effect to a fundamental right.

---

[128] See Case T-135/09 *Nexans*, supra fn. 121, and Case T-462/12 R *Pilkington*, supra fn. 123.

[129] The "fruit of the poisonous tree" is a metaphor in the used to describe evidence that is obtained illegally: if the source of the evidence or evidence itself (the "tree") is tainted, then anything gained from it (the "fruit") is tainted as well. The term fruit of the poisonous tree was first used in US Supreme Court's *Nardone v. United States* judgment, 308 US 338 (1939).

Given the importance of the fundamental right to data protection (and privacy) it is more than questionable whether the current Commission's practice is fully in line with data protection law. Regulation 1/2003 does not indicate the scope of the Commission's discretion or the manner of its exercise, in relation to inspections of digital evidence. As Temple Lang correctly points out, this is too important a matter to leave it to explanatory notes, manuals or other non-binding administrative guidance from which the Commission may derogate any time at its discretion.[130] Rather, it would be necessary to establish clear procedures, including for judicial review of the conduct of an inspection, accompanied by effective safeguards against abuse. The public interest in efficiency in inspections and detecting competition law violations should not be used as a pretext for the convenience of the authorities at the expense of data protection law compliance.

Data protection compliance in the context of investigations is not always easy, but with its Privacy Statement and refined Forensic IT procedure and workflow, the Commission has already taken steps into the right direction. Companies are well advised to follow suit and to anticipate the data protection implications of compliance programmes, whistleblowing schemes and investigations in the context of competition law enforcement. They should proactively address these issues so as not to be confronted with them for the first time when a competition authority knocks on their door or in the middle or at the end of an internal investigation. Rather, companies should build data protection considerations in their compliance programmes, internal audits and investigation procedures. Properly drafted privacy policies and notices, complemented by investigations procedures and a particular IT system that distinguishes between business and private records, can greatly facilitate monitoring and access to certain records including in the framework of investigations. Companies that have implemented a comprehensive data protection compliance programme will usually find that they already comply with many of the data protection law requirements, including with respect to the rules on confidentiality, security, international data transfers and rights of data subjects, and may only need to fine-tune some of the existing compliance tools.

[130] See Temple Lang, supra fn. 4.