Company Data Protection – Friend or Foe?

ANNA WENNÄKOSKI
Former Legal Counsel, currently a visiting LL.M. Scholar

"There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again --."1 Quite a pessimistic view, one might think. Yet, even if one would refuse to undersign any such though-provoking statement as the ultimate truth, one can not totally by-pass it either. Moreover, it could even be posited that some companies might not even acknowledge that they have been victim of a data breach.

For, today, in the midst of the information society we live in, the legal requirements set to data protection should – and can no longer ignored. Phenomena such as globalization, digitalization, outsourcing, fast pace employee mobility, with digital equipment, not to mention various mobile application that collect and track our living habits as well as “Bring Your Own Device” (“BYOD”) –policies, are becoming omnipresent in our daily life. Further, it has been posited that the mankind has probably never produced as much information as does today. At times, the sheer volume of data seems exhausting, not the least from an in-house counsel’s workload perspective. Nonetheless, companies typically have a need to exploit and utilize various data in their respective business and perhaps to further commercialize it too. A start-up business can even be based entirely on a business concept around (personal) data.

All the above phenomena also underline the importance for each organization to recognize and to treat their valuable data as an asset and with due care. A well-organized data protection can also help to protect the company’s intellectual property (“IP”) and also bring added value by promoting the company’s compliance and risk management and thus support the company’s corporate image too. Finally, research seem to indicate that there would be data-driven companies would have an output and productivity at least 5-6 % higher than their peers. 2

Yet, from a legal point of view, the rules on data protection have been quite a puzzle. However, during the past few years, we have been able to witness an extensive review of some of these rules– both on an international (regional) level, such as the EU, but also, nationally, as for instance in Russia3, the UK4, Singapore5 and South Africa6, simply to name a few.

In this article, we will focus on how the landscape could change along with two considerable EU-proposals under way, namely a proposal for a directive on the protection

---

1 FBI Director Robert Mueller.  
2 Brynjolfsson, and Hitt and Heekyung Hellen.  
5 Personal Data Protection Act 2012, in force from July 2, 2014.  
6 Protection of Personal Information Act (“POPI”), as approved by the South African president on November 27, 2013.
of trade secrets ("proposed Directive") and undisclosed information\(^7\) as well as a proposal for a data protection regulation\(^8\) ("proposed Regulation"), and measure how these will fit into the way in which data matters are often perceived from a company point of view.

**The EU Proposal on the Protection of Trade Secrets**

Currently, no uniform rules nor concepts on trade secrets within the EU exist (save from the "undisclosed information" as in article 39 TRIPS). Instead, there are various different solutions, since basically each country has its own system of protection.\(^9\) Up until today, companies have typically been struggling to navigate among these inconsistencies.

Taking into account this legal uncertainty, the EU Commission proposed the Directive on the protection of trade secrets in November 2013. Besides the fragmented national field, one can distinguish several other key drivers behind the proposal; the prevention of infringements, digitalization, and securing R&D and innovative activities. To the last mentioned elements, one can also clearly see the connection to competition law, and also perhaps to a need to close closer to its close trading partners (US and Japan). The EU Council gave its general approach on the proposed Directive in May 2014. Thereafter, the Proposal was examined in the committees of the EU Parliament.\(^10\) In any case, the adoption of the Directive will likely be followed by a two-year implementation period.

The proposed Directive includes a definition of the subject matter of protection (1§), and of some other key concepts (2§). It also addresses the issue of the unlawful (3§) and lawful (4§) acquisition, use and disclosure thereof. Finally, it also includes rules on the preservation of confidentiality in the course of legal proceedings (8§), and on corrective civil law measures (6§, 11 §), also on an interim basis (9-10§), as well as rules on damages (13§). However, pessimistically, it could be asked, whether will the Directive remain *de facto* a dead letter, for the mere reason that criminal law remains excluded of its scope?

One of the starting points of the Directive would be that there would hence be one common legal definition of « trade secret » within the EU. Within the Proposal, “trade secret” is defined as information which meets all of the following requirements: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.\(^11\) To a great extent, this definition would be based on the definition of undisclosed information as in the TRIPS agreement.\(^12\) This would, with much likelihood, render the following implementation easier in Member States. However, the requirement of “reasonable steps” to ensure protection to the data underlines that some active course of conduct by the company will be needed. Moreover, as with the forthcoming new EU regulation on the protection of personal data, it can be envisaged that the “paper trail”

---

\(^7\) Proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure - 28 November 2013/813 final.


\(^9\) See the EU Study, p. 4 and see also the Citizens’ summary.


\(^12\) See TRIPS agreement, article 39(2).
will become more and more important, not the least for good compliance’ sake. We will revert to that aspect later on in this article.

Now, in essence in the Proposed Trade Secret Directive, it is expressly recognized that acquisition, use as well as disclosure of a trade secret can be unlawful. Regarding the threshold for liability, the most important element in the Proposal would seem to be the lack of consent of the holder of the trade secret. Further, it is important to note that besides willful acts, also unintentional ones can become unlawful, since “knew or should, under the circumstances, have known” will be enough to impose liability. This is important since also “passive receivers” i.e. such person(s) who receive the trade secret basically in good faith to begin with, could hence become liable.

Chapter III of the proposed Directive establishes the measures, procedures and remedies that should be made available to the holder of a trade secret. Both civil enforcement instruments and interim measures are at the disposal of the injured party. Here too, the wording is obviously inspired by the TRIPS but also of the Paris Convention. The measures referred to in the Proposal shall at least include the possibility to restrict access to documents and access to hearings, and a possibility to make available a non-confidential version of the related judicial decision.

In accordance with the main doctrinal view, the purpose would, however, be not the creation of exclusive rights. Thus, several companies would still remain able to exploit similar kind knowledge as “their” trade secret. Further, as exceptions, the Directive would expressly recognise independent discovery and reverse engineering, as well as «any other act which is in accordance with commercial practices » as lawful ways to exploit such data. Despite its broad wording, this article would likely be absolute harmonisation.

All in all, however, as the majority of these provisions would be of minimum harmonization only, the proposed provisions also seem rather vague, certainly good to encompass a wide variety of industries and practical situations, yet, however, also subject to legal uncertainty.

The (national) implementation(s) of the proposed Directive remain open. Several options could be envisaged. Whereas in some member states, such as Sweden, there is already today one single act bringing unity and legal certainty to this central issue, in some member states, the legal rules on trade secrets are currently rather scattered in various laws. In such case, the harmonisation could also remain somewhat challenging. A certain dynamic of the EU will likely be included to this too, since the national solutions can vary to some extent. What remains under EU law and national law remains to be determined too.

Be it as it may, the Directive as such offers a great opportunity for companies to review their practices regarding the creation and dissemination of data and knowledge. Do each

13 Proposed Regulation, preamble 65 and article 28.
14 Proposed Directive, article 3(1).
20 TRIPS, article 41.
21 Paris Convention, article 10ter(1).
22 Proposed Directive, article 8.
24 In Sweden Lag om Skydd för företagshemligheter 1990:409.
employee become aware of and acknowledge sufficiently what is considered as company valuable and sensitive data within the organisation? Do each employee sign a separate NDA or is confidentiality included as default in the employment agreements? In these respect, the proposed Directive would certainly not render futile appropriate wordings in agreements and contracts. The latter ones will likely remain at least complementing the Directive, since despite the transition period, it could take years before accurate case law on the proposed Directive will be finally established.

In the mean time, a data protection audit ("due diligence") can help as a first aid. After that, revisions of some contract templates could seem justified, at least once the proposed Directive will have entered into force. Other practical considerations which remain are at least database access rights (passwords, encryption, watermarks, logs, etc.), retention, and finally also access to physical premises (e.g. production sites, laboratories etc.). At least in-house counsels working among these tasks will likely not fall short of work any time soon.

**Part II Protection of Personal Data**

The current EU legislation on personal data dates back to 1995. After that, a lot has happened. The collection of data has, not only become much more widespread in volume but also in terms of methods in which data can be collected and analysed. Entire businesses also thrive today revenues from mere extraction and / or analyse of data.

In 2012, the EU Commission set forth a larger data protection reform in the EU. The goals of this reform too remind us of those for trade secrets as above: to respond to globalization and new technological challenges and to harmonise data protection rules within the EU, but also to strengthen the fundamental right to data protection, to safeguard online privacy rights, reinforce data security and boost the digital economy in Europe and thus indirectly also competition.

Following that, the EU Commission published a first (draft) regulation on the protection of personal data already in January 2012. Only in June 2014 – and following lengthy debates - the European Parliament adopted its view. Finally, in June 2015, the Council of the EU agreed on General Approach to the proposed Regulation. Basically, the Council’s text will set the basis to the final “trilogue” negotiations with the European Parliament and the Commission. The trilogue meetings with the view to reach final agreement are now underway and it is envisaged that a final text of the Regulation could be reached by the end of this year.

One of the central aspects in the proposed Regulation are so called “Privacy by Default”; and “Privacy by Default”, which set as starting point that privacy is taken into account in the planning and production phase already. Accordingly, personal data issues would hence need to be taken care of on a “built in” –basis; i.e. not sporadically afterwards.

This also likely underlines the central significance of risk assessments. To that, when the processing is likely to result in high risk for data subjects, it would hence become mandatory to carry out a privacy impact assessment “PIA”. The definition of what

---

25 Nonetheless, whether we are talking of a violation of law or of a contractual infringement would naturally have an impact into the consequences thereof.
30 Proposed Regulation, article 33.
constitutes “high” or “low” risk would remain under the power of (national) data protection authorities to define.

From a practical point of view, the newly refined rules have an impact not only to lawyers, but to engineers, privacy champions alike. They could also impact for instance “RFP”-tendering processes; i.e. well before the launch of a new product, since these issues would need to be taken into account there too. However, again, taking into account the agile and at times extremely fast pace of the business environments today, such assessments may sometimes seem excessive, if not exaggerated, or simply impossible to perform each time altogether. However, at the end of the day, well-planned products and production phases benefit both the company and its clients.

However, on the other hand, mere PIAs in connection of an individual process or product launch could not be sufficient. To that, auditing, involving more regular follow-up, would render possible the more natural adoption of data protection into the entire organization (for instance by adopting it into the internal audit processes) and again, underline that data protection should not be viewed as a one-time project only, but as a continuous process.

All in all, the advantages for businesses arise largely from the ways in which the data collected can then in practice be used. To that, often the concept of “data flow” (from one system to another) is crucial. However, such systems do not necessarily work (on a stand-alone basis or jointly together) in an optimal manner to classify or to protect trade secrets. To those, human “intervention” is at least necessary to begin with. For, despite the immense amounts of data gathered, not all of it is necessarily commercially nor strategically relevant at all.

Regarding the revisions proposed by the EU Council, the Council seems to take a risk-based approach to compliance. Such an approach, reflected in particular throughout Chapter IV of the Regulation, can allow data controllers to exercise greater discretion and flexibility in assessing their compliance responsibilities within their particular businesses. The wider aim of the Council has been to aim to reduce the administrative burden (e.g. that notification obligations could be lighter). Not for certain, however.

At least the “legitimate interest” will likely become much more regulated. Also many of the great principles upon which the European data protection laws are already today based on, will likely remain too. These include among others lawfully, fairness, a valid legal basis for data processing, as well as transparency. Will the new rules enhance privacy, remains to be seen, however.

At least it has been envisaged that personal data should only be processed if the purpose of the processing could not be fulfilled by other means. I.e. in this respect, the regulation would include a duty to minimize the processing of personal data; i.e. in case an assignment can be performed without personal data, it would need to be done typically.

33 As examples can be mentioned the requirements of privacy by design and by default (in Article 23), the appointment of a representative in the EU for processing activities that are “occasional” and “unlikely to result in a risk” to the rights and freedoms of individuals (preamble 63 and Article 25), unless the national law of the relevant Member State provides otherwise the level of security measures that are considered “appropriate” (Article 30) as well as regarding data protection impact assessments (Article 33). https://www.huntonprivacyblog.com/2014/10/articles/council-european-union-proposes-risk-based-approach-compliance-obligations/.
34 Proposed Regulation, preamble 38.
35 Proposed Regulation, preamble 30.
Data security issues are addressed in the chapter 2 of the proposed Regulation. Article 30 would oblige the controller and the processor to implement appropriate measures for the security of processing, based on the current Directive 95/46/EC.36

What is more, the Regulation would i.a. rely on the neutrality of technologies,37 and apply to “processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system.” However, it appears rather curious that “-Files or sets of files as well as their cover pages, which are not structured according to specific criteria” would not fall within the scope of the proposed Regulation.”38 Yet, data portability39 (i.e. to transfer data from one electronic processing system into another) has been one goal too.

In any case, when collecting and processing sensitive personal data, consent from the individual concerned would need to be explicit. However, further processing would be permitted where it is “compatible” with purposes for which the data are collected. To that, in case consent is duly obtained (or such a set-up is based on contract) and the personal data processed in a machine-readable, structured and commonly used format, the data subject has the right to transmit such data to another controller without hindrance from the original controller.40

In case a requirement of an explicit consent would become a norm, standard terms and conditions offered by companies will likely not be enough. In any case, corporate policies will in any case likely have to be reviewed. Some crucial questions however remain unanswered, however. How, e.g. will be treated a situation wherein a consent is later cancelled? Under which rule would intra-group transfers qualify? Etc.

Regarding the aim to promote the data subject’s rights,41 we can mention for instance the “right to be forgotten”42 (or “right to erasure”)43 as well as the right not to be subject to automated profiling that the Regulation would purport. These could generate increased demands from individuals at least.

Further, following the in-famous “Google decision”44, the right to erasure, also known as “right to be forgotten” will likely be enshrined in the proposed Regulation too. Basically, a controller would then be obliged to erase personal data without undue delay in case such data is no longer necessary for the original purpose or the data subject objects (unless an exception would apply).45 Although seemingly justified for democracy and individual rights, the expanded right to object could sometimes demand considerable human and technical measures from organizations too. One single such demand could in practice be rather arduous.

However, it is also noteworthy that in « General approach » of the Council, the draft proposal was amended so that it now hears explicitly that data protection is not an absolute right but must be weighted against other fundamental rights.46

---

36 Proposed Regulation, p. 10.
37 Proposed Regulation, preamble 13.
38 Proposed Regulation, preamble 13.
39 Proposed Regulation, article 18.
40 Proposed Regulation, article 18(2).
41 Proposed Regulation, article 14 and 15.
42 Proposed Regulation, article 17.
43 Proposed Regulation article 20 and preamble 58.
44 Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Not yet published in the OJ.
45 Proposed Regulation, article 17.
46 See the Council’s notes 10227.
Further, one could also ask, how will the “right to be forgotten” be executed in cloud services?

The rules relating to cross-border data transfers could be clarified, yet not perhaps as much as was initially envisaged. To these, the “adequacy” requirement\(^ {47}\) would likely still remain. Also existing EU model clauses would remain effective, until decided otherwise by the Commission. Further, supervisory authorities would not be able to require prior authorizations to transfer on this basis. In addition, binding corporate rules (“BCRs”) could be available for both controllers and processors.\(^ {48}\) Finally, also seals and certifications could be purported too. For transfers to a non-EU country, a notification and prior approval could become the rule.\(^ {49}\) In any case, it would appear necessary for various businesses to review and verify their data transfer rules.

All in all, choosing a data transfer mechanism can be highly strategic too, relating to how a company defends its business and develops its organisation. Typically, it may well be that a single transfer mechanism alone is not sufficient; instead, various mechanisms can be combined too. The new mechanisms, i.e. above all standard contractual clauses, certification mechanisms, and privacy seals, seem to respond to a public outcry for providing the operators with more flexibility, while allowing them also to demonstrate compliance. However, there is of course, a challenge of how to ensure consistency and, at the other end, a danger of losing legal certainty.

Be it as it may, the role of a data protection officer (“DPO”) could become much more regulated. It remains, however, still open, whether such a nomination should be optional unless mandatory under a national Member State law\(^ {50}\) (as suggested by the Council) or obligatory (Commission and Parliament texts, which would make the appointment compulsory, subject to certain thresholds).\(^ {51}\)

Based on the establishment of the ‘one-stop-shop’ mechanism,\(^ {52}\) a single data protection authority (DPA) (as that DPA where the company has its main base) would be responsible for treating the request of a company operating in several countries.\(^ {53}\)

Other remarkable changes that the new Regulation would bring could include an overall increase in the documentation and notification duties. Also co-operation is likely to be increased.\(^ {54}\)

The Regulation could apply to both businesses established in the EU and to non-EU businesses offering goods or services to individuals within the EU or monitoring their behavior.\(^ {55}\) Obviously, such a broader territorial scope, providing EU data protection authorities with a right to interrupt into businesses based outside the EU, has been subject to some controversy, especially by non-EU based entities.

It can be somewhat regretted that the EU proposal seems rather silent on many other practical questions too, such as data retention.\(^ {56}\)

Further, in terms of trade secrets \textit{stricto sensu}, the Regulation would merely state that the ‘members and the staff of the supervisory authority shall be subject, both during and after

\(^{47}\) Directive 95/46, article 25.
\(^{48}\) Proposed Regulation, article 43.
\(^{49}\) Proposed Regulation, article 43a.
\(^{50}\) Proposed Regulation, article 35.
\(^{51}\) Proposed Regulation, article 52.
\(^{52}\) Proposed Regulation, articles 29 and 34 and 45, 55, and 56.
\(^{53}\) Proposed Regulation, article 3(2).
\(^{54}\) Cf. with the US Fair Credit Reporting Act Publ L. No 90-32 15 USC § 1681 et seq.
their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties”. 57

A data breach notification to the competent data protection authority would likely become mandatory. 58 In case in the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider would be obliged to notify also the subscriber or individual of the breach. 59 It can be estimated that such notifications will likely become challenging to perform sometimes. At least the related administrative burden could be significant.

In case the company uses another provider to perform part of a service, (for example for invoicing), this service provider, which has no direct contractual relationship with the end user should not be obliged to issue notifications in the case of a personal data breach. Instead, it should alert and inform the provider with which it has a direct contractual relationship. This should apply also in the context of wholesale provision of electronic communications services. 60

In terms of liability, based on the new rules, also processors – i.a. not only controllers, could become jointly and severally liable too. Thus, there even direct processes against processors could be envisaged. However, also joint and several liability with the controller would remain, but it could be denied in case the processor or controller proves that it was not responsible for an event giving rise to the damage. To that, at least organizations that act in both as a controller and as a processor may need to keep separate tracks. This could be laboursome, to say the least, especially if one would need to start such organizing from scratch.

Yet, the price tag for a cyber attack could amount to such high figures that the consequences could be insurmountable. 61 This could be the case especially, in case the maximum penalties for non-compliance could raise up to €1 million or 2% of global annual turnover, as envisaged in the Council’s revised text (Although this can, of course, also be seen as a significant reduction from the original €100 million / 5% figures proposed by the Parliament), these figures remain still substantial. 62

It can be noted that once the proposed Regulation would enter into force, the current directive on the protection of personal data 95/46/EC would be repealed. 63

All in all, and fully acknowledging that a considerable amount of the proposed Regulation is still subject to change as the Trilogue negotiations pursue forward, it can, however, already be predicted that several companies would have to perform quite extensive review and perhaps also amendments regarding their current data processing and transfer rules and practices. It can be speculated that full compliance with such new obligations would seem to require substantial resources also from an organizational perspective. Yet, organizations may simply need to launch new intra-company data protection rules too.

57 Proposed Regulation, article 50. See also proposed article 84.
58 Its further details are still debated; for instance the Commission has proposed a deadline of 24 hours; the Council “within 72 hours” and the Parliament “without undue delay”. See proposed articles 31 and 32.
59 Regulation 611/2013, article 3.
60 Regulation 611/2013, preamble 18.
61 The survey was conducted by the Ponemon Institute among 257 benchmarked organizations. According to the survey, the average annual cost in damages from cyber attacks amounted to $7.6 million dollars. See Ponemon Survey.
62 Proposed Regulation, article 79.
63 Proposed Regulation, article 88.
Now, based on the above, it can now be asked, whether organizations are prepared enough; do they have the abilities and recourses to defend themselves against the cyber threats? How are rights to databases etc. allocated and managed? Finally, what about data retention and destruction? Several challenges seem at least to lurk organisations in the pipeline.

**First challenge: Identification & classification**

In practice, a typical challenge is, firstly, that sensitive data is nearly not always recognised within organisations. This can lead to undesired consequences. In that, it may sometimes turn out helpful to ask some key questions, such as what information is important and valuable for your business? Customer data? Intellectual property related data, such as drawings, technical specifications, etc.? And what have you done to ensure their protection?

Once identified, the data amounts would then need to be classified too. Not such an easy task either. Are we talking about personal data, customer data, pseudonymous data or statistics etc. For what is more, one can not know for certain that similar data would necessarily be classified similarly in different jurisdictions. For instance, pseudonymous data has not always been viewed as subject to privacy laws in the US; whereas different views have been expressed in the EU. To that, one can also wait impatiently on the final wording within the proposed Regulation.

Further, it appears somewhat twisted that at times, focus has sometimes been that extensively – if not exclusively – on technical aspects only. True, they are absolutely not to be neglected, and for sure, there are for instance, rather uniform standard rules available.\(^64\)

Yet, despite the fact the organization might have made considerable investments into providing technical security, the organizational culture in terms of privacy matters can have remained rather thin, if non-existing at all. People within organizations do not perhaps recognize the relevant issues at stake and those issues might then pop up in surprising occasions and both pose an additional vulnerability. Without doubt, both education and training are needed, to say the least. In addition, the entire lifecycle of information would need to be taken into account, and viewing data protection as a continuous process\(^65\), not as a one-time project only. In that, the new “data protection officers” could definitely bring some help in fostering an organization culture that supports data protection.

For, at the end of the day, what matters greatly is also the personal attitude amongst each employee. For even the greatest of internal policy or instruction can render an organization immune from data breaches – be them in terms of trade secrets or personal data *sensu stricto*; in case its employees and managers are ignorant of the critical assets or on the rules and mechanisms surrounding their protection.

True, the legislation for sure leaves room for ambiguities too. Yet, it would seem most natural to include data protection into the normal prudence requirements within the corporate duties, such as the duty of care and duty of loyalty. From that perspective, data protection should be part of the job description for many corporate officers, similarly as for legal advisors, accountants and doctors. In that, we can definitely see that the data

---

64 See e.g. the International Organisation for Standardization and the International Electrotechnical Commission, which has i.a published the often times solicitated “ISO/IEC 27001” standards.

65 See also the ISO 31000 standard.
protection “culture” is – or should be – to an increasing amount also a management issue, I posit.

Second challenge: Ownership and Use

Secondly, even though the company would claim to be fully aware of its valuable data, it then faces the other crucial question of who owns such data and what can it do with it – both intra company as well as in relation to business partners.

Intra-company, relevant questions are at least:

- to which function /team does the entire responsibility (ownership) of data protection and privacy matters belong to? Legal? Compliance? Information management or Information Security? R&D? Human Resources? The mere multiplicity of choices serves as testimony of the multiple faces of the topic itself.

In relation to business partners:

- To which party are the end result of a certain collaboration allocated to?
- And can the other party/parties licence options to that?
- Are there data transfer agreements and clauses in place?
- How are the data sharing practices organised?

Despite that many corporations would have privacy matters well organised on a head-quarter level, local ownership of data – or the of it – can also become a risk. To that, also whistleblowing policies and practices can help too.

In many respect, it would appear justified and practical to align trade secrets into the general IP strategy of the company too. That could also bring answer to the question of who/which team is responsible for trade secrets’ instructions too. Needless to say, we are tempted to find the most efficient solutions. No “one-size-fits-all” solution seems available, however.

Finally, needless to say, also budget related considerations are in practise often meaningful. How much resources are dedicated to data protection matters and/or to certain project thereto? Needless to say, now in relation to the up-coming legislative changes, various commercial actors, be them of data security, cyber insurances, metrics, analytics etc. do not miss their chance in selling eagerly their services to companies. To these, companies should exercise prudence in choosing their “must-win-battles”.

Third issue: organising the protection in practice

It should go without saying that no sector is safe from the challenges brought along by the cyber environment and the rise of data as a critical asset. However, looking at the most costliest cyber attacks in our modern time history so far, it seems that the financial and banking data is rather exposed.

In practice, mere case investigations can also rapidly raise rather high; forensic experts, external advisors, let alone court and dispute resolution proceedings are often rather lengthy timewise and can require substantial resources. Further challenges relate to requirements of evidence in court. These can impact also on companies’ willingness to initiate a proceedings to begin with.

If one succeeds to find such evidence and winning arguments, at the end of the day, a court judgement can pronounce the violation and breach of data. Also damages can be allocated. However, exact estimates of the total damages can be challenging; how to for

instance measure future harm? To that, the proposed Directive could render the situation better.\textsuperscript{67}

One of the most important tasks is the raise awareness on these issues and to define the roles and responsibilities adequately.

Most importantly, businesses should be aware of the level of the scrutiny within the upcoming legislation. It can even be asked, how smaller companies (within the scope of application) will be able to bear the costs of the organizational and contractual etc. changes that the proposed Regulation is likely to cause. Having said that, it could well be – as it already can be the case – that these issues have a major impact to companies’ strategies too.

Further, the practice of using third parties in the processing of data has proliferated amongst companies. Needless to say, consultants, suppliers and sub-suppliers, (cloud) service provider(s) may also need such information in order to perform their work. To that, despite the advantages therein, also several risks remain, i.a. data being used for other purposes than that to which such external party originally received the assignment, not the least due to varying national standards. Finally, it comes down much to a balancing exercise between what is necessary to be protected; and what needs to be disclosed. How to manage necessary access; without providing too much? If viewed from the perspective of a controller, it would be useful to have the business partner (e.g. a supplier /vendor) acknowledge his position as a data controller. Yet, this is in practice not often the case. And this complicates matters and upholds an in-balance in terms of the liabilities. Typically, cloud service providers limit considerably their liabilities; thus, the risk remains at the company giving the assignment. This can also affect on what kind of data e.g. companies are willing to place in a “cloud”. However, advantages related to cost-efficiencies, and scale-advantages, in addition to faster response time, can still weight considerably too.

Alas, also economic analysis is sometimes needed too, however. Economic theory does not, however, succeed in providing us a clear answer to the question “how much control is optimal”.\textsuperscript{68} Neither is there any “economic policy” which would provide the holders of such information guidance on the optimal level of undisclosed information. The question, however, on how to organise these issues in practice, is to be left for the economic operators to be decided, since no « one solution fits all » seems appropriate.

\textbf{Some Final Remarks}

Finally, today, it can be claimed at least that a) knowledge and data equal power; b) mastering the management of such data will allow companies to thrive increasingly within their own businesses; and c) to that, the legal requirements set to data protection should – and can no longer ignored.

To an increasing amount, data protection rules will hence likely be harmonized in the EU – apart from employee rules that will remain national.

Understanding the new rules demand for both prioritising and education. To these, the above EU – and other legal reforms within the field of data protection, offer, all in all, a great opportunity for a learning exercise for organisation, to review their practices, to update their knowledge and to raise awareness on data protection; a legal order which, for certain, will not likely remain silent in the near future.

\textsuperscript{67} See proposed Directive, article 13.
\textsuperscript{68} Lemley 2004, p. 43.
***

Anna Aurora Wennäkoski (LL.M. and M.Sc.) is an internationally-oriented lawyer, specializing in intellectual property rights (“IPR”s), information law and data protection. Her master’s thesis on IPRs was selected winner of the American Resource Center research award. Within her day-to-day work as a legal counsel, Ms. Wennäkoski has worked for several years in stock listed companies at the vanguard of Scandinavian business and in France, and among various IPR and data protection matters. Currently, Ms. Wennäkoski is preparing post-graduate studies in New York, US.
Sources

Agreement on Trade Related Aspects of Intellectual Property Rights, as Annexed to the Marrakesh Agreement establishing the World Trade Organization, signed on 15 April 1994 (TRIPS)

Paris Convention on the Protection of Industrial Property of March 20, 1883, and as later amended (Paris Convention)


EU Council’s comments to the Proposed Regulation Inter-institutional File: 2012/0011 (COD) 10227/13 Brussels, 31 May 2013 (Council’s notes 10227)


Other legislation

US Fair Credit Reporting Act Publ L. No 90-32 15 USC § 1681 et seq.

Case law

Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Not yet published in the OJ.

Articles

FBI Director Robert Mueller: “FBI Director: Cybercrime will eclipse terrorism” available at
http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/ March 2, 2012 (Robert Mueller)


Ponemon Survey

Other