Cyber liability: Data breach in Europe
Data Breach

Cyber Attack
How often has your data been hacked? Have you received a notice from your bank recently about suspicious transactions? Have you already adapted to the "new reality" of data (in)security?

Although the topic of cyber security is much broader than the data breach example, the media focus is usually on data breaches, which occur at a much higher frequency than other cyber events. Because data breaches also, so far, generate most of the cyber-related insurance claims, we limit the scope of this publication to those types of events.

While data breaches might have become commonplace, their effect on the breached entity (and the affected individuals) are often far-reaching. The majority of the headline-making data breaches have occurred in the United States. But cyber attacks are a global issue, affecting the economy worldwide. New legislation in the European Union is expected to lead to more reported cyber events also in Europe after its implementation in 2018.

This publication looks at the consequences of a data breach in Europe and compares the situations in Europe and the US with regard to the major features of such an event. It provides a snapshot of where the discussion stands at the beginning of 2017, about one and a half years before the new European General Data Protection Regulation (GDPR) will come into force. Watching the case law developing, in particular in the UK which has taken some landmark decisions in this area, is also an indicator for where Europe seems to be heading. The UK intends to implement the GDPR in spite of Brexit.

The cyber insurance market is growing constantly, but the penetration of cyber coverage is still small relative to the value of the tangible and intangible assets that could be impaired by a cyber security breach. According to an AON/Ponemon study, only around 12% of information assets are currently covered by insurance.

---

2 See transcript from UK Parliament: https://hansard.parliament.uk/commons/2016-11-07/debates/1611071000004/InformationCommissioner%E2%80%99sOfficeTriennialReview#36WS. While the UK implements the GDPR as planned, changes are possible after the country leaves the EU.
Background

What is a data breach and why is coverage so critical?

One of the current problems for data owners is that they often have no control over where their data actually goes. Service providers manage the data, and many of these providers use sub-contractors for certain tasks. This is the reality of the connected world in which we live: data is stored in different places way beyond the control and the reach of the data owner’s judiciary. The perpetrators’ methods are similar, irrespective of where the data breaches occur. The targets of such cyber-attacks are often companies that store large volumes of data for themselves, or for third parties.

The most frequent data breaches involve personal information like names, addresses, credit card and account numbers, health insurance numbers, PIN-codes, Social Security numbers and other financial information of a large number of individuals. It’s important to note that although laws give a definition of what personal data is (usually any information allowing to identify the person directly or by combining data elements), these laws keep changing, and courts around the world continue to broaden those definitions. For example, a zip code has been considered personal data, and so has a person’s browsing history on Google. Furthermore, the European Court of Justice decided on 19 October 2016 that IP addresses may now also be considered “personal data”.

A “breach” of such data takes place when unauthorised individuals view, copy, steal or use such information in any other way.

---

5 Microsoft successfully challenged a US warrant seeking e-mails stored on a server in Dublin, Ireland. The case defined for the first time the limited reach of US warrants when it comes to data stored outside of the United States. However, the decision does not limit the government from seeking assistance from the country where the information is hosted by way of judicial assistance.


Who are the (h)actors and what are they after?

Hackers’ motives can be several, such as fun, political, religious, or — presumably most often — financial gain. Behind most of the publicly disclosed cases (eg Target, Home Depot, Ashley Madison), these unauthorised individuals were supposedly professional hackers. The so-called “dark net” has become a lively market place for stolen data that can be used for identity theft, credit card fraud and other criminal activity.

Identity theft is when criminals use someone’s name, credit rating, health insurance number or any other stolen data to gain a financial advantage in that person’s name, including obtaining goods, services, credit or other benefits.

Credit card fraud is a particular form of identity theft, involving a payment card as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorised funds from an account.

Extortion cases are not limited to so-called distributed denial of service attacks (DDoS), but also take place in connection with data breaches. In such cases, the hackers steal data and threaten to disclose it publically unless a certain sum of money is paid, usually in bitcoins. This is often easy and quick money for the hackers because they don’t need any infrastructure to “monetise” the stolen data.

Cases of cyber espionage, including IP theft, whether against private companies, states or governmental institutions, take place, too, but rarely become public. Usually, these situations do not give rise to large insurance claims. This publication, therefore, does not look at such events.

---

8 But this is not always true: one of the most publicised European data breaches, the hack of the broadband firm Talk Talk, was committed by a 16 year old teenager who wanted to impress his friends. http://news.sky.com/story/boy-17-admits-hacking-offences-linked-to-talktalk-attack-10658405

9 The “dark net” mainly consists of webpages which are both provided and can be accessed anonymously. They are not indexed and hence, can not be found via Google or other search engines. Access is only possible via browsers that support special anonymization technologies. Furthermore, for illicit activity, actors often use web-forums within the dark net, and access to those forums is often restricted to admitted users / conspirators. While there is also a lot of legitimate activity such as information sharing platforms for journalists, whistleblowers, political chat rooms, instant messaging services, artist platforms, the dark net has become infamous mainly for the illegal activity which takes place there. The currency used is normally bitcoins. http://www.abc.net.au/news/2016-01-27/explainer-what-is-the-dark-net/7038878

10 In the case of credit card fraud, the person whose data has been stolen usually does not suffer a loss because the fraudulent transactions will not be charged to him/her but rather picked up by the banks and credit card companies participating in the transaction.

11 Amounts are usually relatively low (USD 20’000 to 30’000). The total amount paid in ransom globally was estimated at more than USD 1 bn per year by former FBI Agent James Trainor; see Handelsblatt, Düsseldorf, 13 January 2017.
Reaction to a data breach

When an entity is faced with a breach, it is dealing with an immediate crisis. The consequences of losing someone else’s data can be harsh – both for the person to whom the data relates and to the entity which has caused or suffered the breach. The major elements of a breach response include the following:

Forensic investigation: the breached company will require IT specialists to perform a forensic investigation to assess what happened. What data was accessed and/or stolen, start date of the intrusion, whether the hackers are still within the system, how to restore lost or corrupted data, etc. This part of the breach response is similar around the world.

Public relations: it is vital for a breached entity to carefully manage communication with a view to mitigating the reputational damage to the company and potential corresponding loss of business. The economic damages caused by loss of business after a breach have often been far larger than the costs actually spent on the breach response. Poor communication can have a major impact on the company’s reputation and, therefore, the overall loss. This part of the action plan is mainly influenced by the relevant market and less so by the jurisdiction in which the breached entity operates.

Notification: depending on the relevant jurisdiction(s), the breached entity needs to inform the individuals whose data was accessed or stolen. In the US, there are currently 47 different state notification laws which govern timing, content and form of required notifications to the competent authorities and to the individuals affected by the breach. In Europe, notification to authorities and to the data subjects is not yet mandatory. But this will change in 2018 with the new GDPR.

Credit monitoring: the offering of free credit monitoring for at least one year has become standard when sensitive data of US residents has been breached. To ensure no illicit activity using the sensitive data is taking place, the chosen credit monitoring agency will inform the individual if suspicious activity is detected or, generally, when new credit card or bank accounts are opened in her or his name. Credit monitoring is an important safeguard in the US. Credit reporting agencies are tracking a person’s credit history and are normally involved in any new credit application. Accordingly, they are ideally placed to detect suspicious activities in connection with an individual’s credit card or bank account.

In Europe, however, credit monitoring activities are restricted by law in most jurisdictions and, therefore, a person’s “credit history” cannot be tracked and used in connection with other commercial transactions. As a result, there are no institutions comparable to the US credit reporting agencies where different transactions in a person’s name can be systematically scrutinised for suspicious activities. Therefore, US-style credit monitoring cannot be offered in Continental Europe and, as a result, does not create such breach response costs. Some vendors in Europe, however, have started to offer so-called “web monitoring” which includes scanning the Internet and the dark net for sensitive personal data of affected individuals. If such data is found, the individual receives an alert which will allow him or her to take action such as informing his or her bank, or other companies, to prevent fraud. The UK is the European exception: credit monitoring is common and routinely offered in connection with data breaches in the UK.

12 For the costs of a data breach in the US, please see: “Cyber Liability. Features of a data breach”, 2016, page 2 et sec. http://www.swissre.com/library/Cyber_liability_Features_of_a_data_breach.html. In Europe, the experience with breach response cost is not yet as broad while at the same time the law and the vendors’ market is still developing.


14 In France, for example, creating black lists is forbidden by law. Only the “Banque de France” is allowed to get information about people’s “incidents de paiement” (debts). The Banque de France is then allowed to share this information with credit companies / banks (arrêté du 26 oct. 2010 relatif au fichier national des incidents de remboursement des crédits aux particuliers)
The consequences of a data breach are materially influenced by the legal landscape in which the breached entity is operating.

While there are several federal data security and breach notification bills pending in the US Congress,\textsuperscript{15} at the time of writing, a variety of federal and state laws still regulate the topic in the US.\textsuperscript{16}

Europe, on the other hand, is facing major changes in data privacy law with the GDPR,\textsuperscript{17} that will come into force on 25 May 2018. The GDPR applies directly and will replace all existing national data protection laws in the EU Member States.\textsuperscript{18} Another piece of relevant recent EU legislation is the Network and Information Security Directive (NISD) adopted on 6 July 2016. The NISD is a “Directive” and, therefore, requires implementation by the EU Member States into their national laws, which should take place within 21 months from its adoption, ie by May 2018.

The two legislations are complementary initiatives with the common goal to modernise and harmonise the data protection frameworks across the EU. The purpose of the NISD is to enhance online security in the EU and thus goes beyond data protection only. It applies to operators of essential services\textsuperscript{19} and digital service providers.\textsuperscript{20} The GDPR focuses on protecting personal data wherever and however it is stored. It applies to anybody who is storing or processing data of European data subjects, including data processors located outside of the EU. Accordingly, the GDPR is expected to have the most direct impact on future data breaches. Therefore, in this publication, we focus on the impact of this new legislation, which is mainly expected in the field of notification requirements and regulatory fines.

\textsuperscript{16} For the 47 different state laws that apply to notification, see: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
\textsuperscript{17} http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
\textsuperscript{18} For a list of the current EU Member States, please see: http://en.strasbourg-europe.eu/member-states,3322,en.html
\textsuperscript{19} The NISD defines the operators of essential services as the entities which provide a service which is essential for the maintenance of critical societal and/or economic activities. EU Member States are required to identify operators of essential services; these will include the energy, transport, financial services (inc. banks), health, and digital infrastructure related industries.
\textsuperscript{20} Digital Service Providers are providers of online marketplaces, online search engines or cloud computing services.
In Europe, except for certain industries (e.g., telecom), there is currently no mandatory obligation to notify a data breach. This could explain why there are much fewer reported data breach cases in Europe compared with the US. But fewer reported cases does not necessarily mean that data breaches do not regularly occur in Europe as well. Some have made the headlines and have increased awareness of this topic also in Europe.\footnote{For examples of EU data breaches, please see the presentation of Elena Jelmini Cellerini and Catherine Lyle of January 2016: http://media.swissre.com/documents/Presentation_Catherine_Lyle+and_Elena_Jelmini_Cellerini1.pdf}

Under the GDPR, notification of a breach to the supervisory authority becomes mandatory in all cases where the breach poses a risk to the rights and freedoms of natural persons (art. 33 GDPR). Notification to the affected data subjects, however, is only mandatory where there is a high risk to the rights and freedoms of natural persons (art. 34 GDPR). Unfortunately, the GDPR does not contain a definition of “risk” and “high risk”. Time will tell what direction the European regulators and ultimately courts will take with regard to this distinction.

Please see the table below for a summary of the requirements of a notification under the GDPR:

<table>
<thead>
<tr>
<th>Risk to the rights and freedoms of natural persons</th>
<th>Notice to Supervisory Authority</th>
<th>Notice to Data Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>mandatory</td>
<td>not mandatory</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High Risk to the rights and freedoms of natural persons</th>
<th>Notice to Supervisory Authority</th>
<th>Notice to Data Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>mandatory</td>
<td>mandatory</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Timing</th>
<th>no later than 72h</th>
<th>without undue delay</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Content</th>
<th>a) nature of personal data breach; categories and number of affected subjects and records</th>
<th>a) nature of personal data breach</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>b) contact details of data protection officer</td>
<td>b) contact details of data protection officer</td>
</tr>
<tr>
<td></td>
<td>c) likely consequence of the breach</td>
<td>c) likely consequence of the breach</td>
</tr>
<tr>
<td></td>
<td>d) measures taken or proposed</td>
<td>d) measures taken or proposed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Form</th>
<th>not defined</th>
<th>not defined</th>
</tr>
</thead>
</table>

| Exceptions from notice requirement | breach is unlikely to result in a risk to the rights and freedoms of natural persons | i) the personal data is unintelligible, such as encrypted, or (ii) if the entity has taken action subsequent to the breach to ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialise, or (iii) when the notification to each data subject would “involve disproportionate effort”, in which case alternative communication measures may be used |

Please see the table below for a summary of the requirements of a notification under the GDPR:
The GDPR authorises regulators to levy hefty fines in amounts as high as 4% of the breached entity’s annual turnover, or EUR 20m, whichever is greater. However, only a few articles of the GDPR deal with data security and breach notification, and only these provisions of the law are relevant in connection with a data breach.\footnote{22} There is ambiguity in the GDPR as to whether a data breach could attract the full 4%/EUR 20m fines or only the lower 2%/EUR 10m fines pursuant to article 83 para. 4 GDPR.\footnote{23} It appears that fines for an inadequate reaction to a data breach are limited to 2% of the annual turnover or EUR 10m (whichever is greater), while the fine for systematic inadequacies in data security could go as high as 4%/EUR 20m. It remains to be seen how the competent authorities and courts will interpret the GDPR in this regard. One way or another, fines of this magnitude must put data security issues on the agenda of every diligent management and board of directors.

Factors taken into account for the assessment of the fines include the following:\footnote{24}
- the nature, gravity and duration of the infringement, the number of data subjects affected and the level of damage suffered by them;
- the categories of personal data affected by the infringement;
- mitigation measures taken by the breached entity;
- previous infringements by the breached entity;
- adherence to approved codes of conduct or certification mechanisms by the breached entity.

Already under the current law, regulators are looking at aggravating or alleviating factors in a similar way.\footnote{25}
Where credit card information is stolen in a data breach, affected credit card companies can impose substantial fines. The merchants or service providers who accept credit cards, and from whom such data may be stolen, have contractually agreed to pay fines and penalties for the loss of credit card information which they hold. The standard contracts between credit card companies, banks and merchants define a complex mechanism for the calculation of such contractual fines and penalties. Penalties are issued for the violation of the applicable PCI standards. The basis for the fines, the so-called assessments, include the operational expenses incurred by the issuing banks for the replacement of the affected credit cards and the amount of fraudulent transactions that can be traced back to the data breach. The individual customer is usually not charged for fraudulent transactions or the replacement of the credit card. Basically, the credit card companies operate by a similar set of such rules in Europe and the US.

26 The Payment Card Industry Data Security Standards (PCI) contain a list of twelve information security requirements promulgated by the Payment Card Industry Security Standards Council, a self-regulating body founded by the five global payment brands – American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. The PCI are the benchmark for all organizations and environments where cardholder data is stored, processed, or transmitted and require merchants to implement a number of measures to protect cardholder data.


Developing case law

In 2016, the UK landmark decision of Vidal-Hall v Google became final and binding when Google withdrew its appeal against it.

The case was about Google’s unlawful practice to store and analyze individuals’ internet surfing history. The decision was particularly important for its finding that (i) a claim involving personal data can be brought without having suffered economic damages and that (ii) emotional distress alone is sufficient to give plaintiffs the right to make a claim in a court of law. This decision is in line with (not yet in force) art. 82 GDPR which explicitly states that “any person who has suffered material or non-material damage ... shall have the right to receive compensation ... for the damage suffered.”

The next important case was the UK decision TLT et al v Secretary of State for the Home Department of June 2016 which, for the first time, put a price tag on such claims for non-economic damages. The case involved the accidental disclosure of 1600 asylum seekers’ personal information. The judge applied Vidal-Hall v Google, finding that compensation for distress arising from the breach was available. The claimants were awarded between GBP 2 500 – GBP 12 500 in compensation per person.

These two decisions show that the UK is following the path taken by the US courts in broadening access to the courts for individuals who have been the victim of a data breach. With art. 82 GDPR not yet in force at the time of the decision, the Vidal-Hall case applied the overarching EU Charter of Fundamental Rights to come to the same result.

While US-style class actions are not known in Europe, different forms of collective redress are on the rise. The Commission of the European Union issued a Recommendation in 2013, suggesting that the Member States should introduce forms of collective redress for consumers. But when doing so, the Member States should avoid the introduction of US-style class actions by, amongst others, permitting only qualifying not-for-profit consumer associations to represent a class. The GDPR follows this same approach and suggests that such forms of collective redress should be available for data subjects under the GDPR. The Member States, however, are free to decide whether collective redress procedures shall be available for claims for damages, or only in connection with non-monetary judicial remedies.

Because a data breach usually affects many individuals in a similar way, they will regularly look towards such collective redress procedures to seek remedy for their injury. If combinable with non-economic damages, like emotional distress, such collective redress actions could change the legal landscape in the respective jurisdiction and materially increase the exposure of breached companies. However, not all EU Member States allow for damages to be claimed in collective redress actions.25

Scope of class actions generally broadened in Europe

While US-style class actions are not known in Europe, different forms of collective redress are on the rise.31

The Commission of the European Union issued a Recommendation in 2013, suggesting that the Member States should introduce forms of collective redress for consumers. But when doing so, the Member States should avoid the introduction of US-style class actions by, amongst others, permitting only qualifying not-for-profit consumer associations to represent a class.33 The GDPR follows this same approach and suggests that such forms of collective redress should be available for data subjects under the GDPR. The Member States, however, are free to decide whether collective redress procedures shall be available for claims for damages, or only in connection with non-monetary judicial remedies.34

Because a data breach usually affects many individuals in a similar way, they will regularly look towards such collective redress procedures to seek remedy for their injury. If combinable with non-economic damages, like emotional distress, such collective redress actions could change the legal landscape in the respective jurisdiction and materially increase the exposure of breached companies. However, not all EU Member States allow for damages to be claimed in collective redress actions.36
The first European collective redress action following a data breach has been filed in the UK. The action, however, is based on the UK Group Litigation Orders procedure which was introduced in 1999. This procedure allows the grouping of cases which give rise to common or related issues of fact or law. The first such action in connection with a data breach in the UK launched in 2015 with the Morrison Supermarket case. As of June 2016, some 6,000 employees opted in, and all claim damages for emotional distress based on the Vidal-Hall decision. The UK group action scheme does not require that collective actions be brought by not-for-profit consumer associations only, which will likely create different dynamics in connection with such claims.

While some aspects of a data breach will be materially different in Europe compared to the US, the table below clearly indicates that the two major legal systems, the US common law and the civil law (which dominates the European Union) are moving closer to each other with the implementation of the GDPR.

<table>
<thead>
<tr>
<th></th>
<th>USA</th>
<th>EU currently</th>
<th>EU in 2018 (GDPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notification</strong></td>
<td>47 state breach notifications laws + multiple proposals for a federal law pending in Congress</td>
<td>Currently only very limited obligations based on national laws</td>
<td>Notification mandatory, with important exceptions (see table on page 6)</td>
</tr>
<tr>
<td><strong>Forensics</strong></td>
<td>No legal obligation, but expected loss mitigation measure of a prudent management</td>
<td>No legal obligation, but expected loss mitigation measure of a prudent management</td>
<td>No legal obligation, but expected loss mitigation measure of a prudent management</td>
</tr>
<tr>
<td><strong>Public Relations</strong></td>
<td>No legal obligation, but expected loss mitigation measure of a prudent management</td>
<td>No legal obligation, but expected loss mitigation measure of a prudent management</td>
<td>No legal obligation, but expected loss mitigation measure of a prudent management</td>
</tr>
<tr>
<td><strong>Credit Monitoring</strong></td>
<td>Required by some state laws – common practice is to offer 1 or 2 years of free credit monitoring</td>
<td>US style credit monitoring prohibited in Continental Europe, but allowed in UK</td>
<td>US style credit monitoring prohibited in Continental Europe, but allowed in UK</td>
</tr>
<tr>
<td><strong>Regulatory Fines</strong></td>
<td>47 state breach notifications laws + several federal laws</td>
<td>Currently only based on national laws</td>
<td>Up to 2% of annual turn over OR EUR 10m, whichever is greater. (Possibly up to 4%/EUR 20m if breach of general principle of GDPR.)</td>
</tr>
<tr>
<td><strong>Contractual Penalties and Fines</strong></td>
<td>Assessed by credit card companies and ultimately imposed on breached entity</td>
<td>Assessed by credit card companies and ultimately imposed on breached entity</td>
<td>Assessed by credit card companies and ultimately imposed on breached entity</td>
</tr>
<tr>
<td><strong>Third party liability: Civil Actions, incl. Class Actions</strong></td>
<td>Individual and class actions. Moving towards admitting claims from affected individuals without proof of material damage</td>
<td>Individual actions, but no US style class actions in EU. Restricted consumer class actions in some states. UK: Vidal-Hall decision allows claims for emotional distress</td>
<td>Individual actions, but no US style class actions in EU. Claims for material and non-material damages admissible. Restricted consumer class actions in some states</td>
</tr>
</tbody>
</table>

### Comparison: Europe vs US

The matter involved an internal auditor who intentionally leaked personal records of 100,000 employees including salaries, bank account details, etc. and posted the information online.
Awareness of cyber risks in Europe remains much lower than in the US. According to a survey conducted by Swiss Re in cooperation with IBM in 2016, 39% of corporations surveyed in North America plan to buy (more) cyber insurance, while only 27% of European corporations have such plans. With only 12% of information assets globally being protected by insurance, there still remains much to do to make our "information society" more resilient. A survey of security professionals indicated that only around a quarter of firms use detailed quantitative cyber risk models, while apparently 60% of companies in Continental Europe have never estimated the financial impact of a cyber loss scenario.

Risk transfer should be one element in a comprehensive cyber strategy. Cyber policies are covering both first party losses and third party liability. The covered first party losses encompass crisis management costs (forensic investigation, public relations, notification, credit monitoring) and regulatory fines, to the extent they are insurable under applicable local laws.

Covered under the third party liability section are basically claims which a breached entity will face, including respective defense costs. Depending on the jurisdiction, the element of defense costs should not be underestimated.

Indemnification for contractual penalties and fines is not necessarily part of the standard coverage. However, cover for these so-called credit card company assessments can be purchased by endorsement, but is often subject to a sub-limit.

Cyber stand-alone policies often also cover business interruption that is directly linked to the data breach. However, loss of revenues after a breach (churning, reputational damage) mostly remains uncovered. Shareholders' derivative actions against directors and officers (D&O) for negligence and breach of fiduciary duties can be the consequence. Even when dismissed, covered defense costs alone can be substantial and, accordingly, D&O policies have regularly come into the focus.

Knowing that IT security is the Achilles heel of companies that process and store personal data, boards are well advised to make cyber security a priority topic on their agenda and review their cyber and D&O cover on a regular basis.

---

The web is worldwide. Therefore, data breaches are a global threat. The response by various jurisdictions, however, has been quite different up until now. With the regulatory changes currently in the pipeline in the European Union, Europe’s and the United States’ way of dealing with data breaches is becoming more aligned. After implementation of the GDPR, the major differences that will remain predominantly arise out of the inherent differences between the civil law and the common law systems.

The possibility to bring class actions creates a dynamic risk landscape in the US. In Europe, we see a cautious opening towards such forms of collective redress, combined with a clear goal to avoid the implementation of a US-style class action system. Moreover, the GDPR grants an unequivocal right for victims to be compensated for material and non-material damages arising out of a violation of the GDPR. Obviously, in those jurisdictions where the combination of claims for non-material damages with forms of collective redress are or will be possible, the risk for breached entities to be held liable for substantial amounts in damages increases significantly.

Another key difference that will remain is that a person’s credit history is still an important feature of the US economy. The use of such data is not common or even prohibited by law in most of Continental Europe. The cost factor created by credit monitoring in the US is substantial, while such losses are very limited in a European case. Only the UK allows credit monitoring activities similar to the US.

The fines under the European GDPR are expected to be much more forceful than those currently imposed in US. The US legal system traditionally gives much importance to the preventive and deterrent effect of private law suits, including class actions. Time will tell whether European regulators will become major players/controllers in the cyber arena, or whether civil actions brought by affected consumers will have the greater impact.
