WINTERHAWK CONSULTING

Helping you prepare for GDPR
One step at a time

Penalties for Non-Compliance with GDPR

When people talk about the new regulations, it's hard not to focus on the fines and penalties facing organisations who don't comply with GDPR. It's easy to see why – the penalties are significantly higher than those set out under previous Data Protection regulations, and by all indicators the Data Protection Authorities (or DPAs) will be under increasing pressure to actually apply them. No doubt the media and companies selling Data Protection related services will use the fines as a hook, and it will most certainly work – we'll see the big numbers reported in the headlines, we'll buy the papers and click the links to" read all about it" – after all, how many of us can resist a big corporate scandal, especially one that's happening to someone else.

Yes, there are reasons to be concerned about the administrative and punitive penalties that could be levied, but there are other potential consequences and impacts we should also be aware of. Let's make sure we understand those headline-grabbing penalties before we get too far ahead of ourselves.

Penalties and Sanctions Levied by the Data Protection Agency

Data Protection Authorities will be pressured to levy significant and deterring fines simply as a warning to others, but this doesn't mean they can or will hand out multi-million Euro fines for simple first offenses or low impact issues of non-compliance. Behind the big headlines, Article 83 (General conditions for imposing administrative fines) specifies the categories of fines and types of breaches which could lead to monetary sanctions.

Category A Fines

This category concerns issues with preparedness and administrative failures in implementing a Data Protection compliance program. It includes but is not limited to:

- Failure to execute a proper Privacy Impact Assessment
- Lacking designation of a Data Protection Officer, or issues with the roles and responsibilities of the DPO
- Issues with Breach Notifications to Data Protection Authorities or to Data Subjects
- Failure to implement Data Protection "by design and by default"

Fines capped at €10 million or 2% of **worldwide** annual turnover, whichever is **greater**.

Category B Fines

Category B generally addresses actual breaches and major failures in compliance. This includes but is not limited to:

- Conditions for consent (in obtaining or processing data, etc.)
- Lawful processing of data
- Right of access by the Data Subject (Subject Access Requests)
- Right of erasure (right to be forgotten)
- Right of rectification (accuracy of legally obtain personal data)
- Processing of a National Identification number
- Obligations of Secrecy

Fines can be up to €20 million Euro or 4% of **worldwide** annual turnover, whichever is **greater**.

This is just a small selection of potential scenarios, and no doubt there will be some that haven't even been dreamt up yet. The bottom line is this: any breach of personal data could lead to a fine.

These administrative penalties are also non-jurisdictional. Much of the point of GDPR is to unify legislation across EU member states, so that the schedules apply equally regardless of where you are in the EU. Moreover, there will be a deliberate effort to ensure that penalties are aligned across member states, to ensure that one state cannot gain a competitive edge over another due to lax enforcement of the GDPR. The regulations will be equally applicable to companies in countries outside of the EU, who process the personal data of EU citizens. While, EEA countries and other "Safe Countries" with formal agreements in place with the EU should pay particular attention to GDPR requirements, technically they apply to *any company* in *any country* dealing with data on EU citizens.

It should be noted that simple first time offenses are not likely to lead to significant (if any) sanctions, and it is clear that cooperating with authorities and proving you have a compliance effort in place will go a long way towards mitigating your risk.

Other Administrative Fines (Member State Level)

There is still some scope for individual member states to levy penalties for breaches related to GDPR, particularly for specific exceptional or criminal breaches in a member state. In general, this is intended to address those items not specifically dealt with by the new regulations and allow member states to fill in the gaps for items falling specifically under local law. For example, many member states differ in their definition of consent as it concerns children/minors, and the EU will continue to allow local enforcement and penalties in accordance with those laws. Furthermore, a Data Subject always has the right to pursue claims against a Data Controller via Civil Suits (Article 82) in their local jurisdiction and in accordance with local laws. The penalties outlined in the GDPR are intended as punitive and dissuasive measures levied against Data Controllers and Processors, but they do not include compensation for damages that the private individual may have suffered as the result of a breach. These matters can be and must be pursued in a separate civil action.

Additionally, in certain member states there is already precedence for finding company Board Members personally liable for serious breaches or issues with non-compliance with existing Data Protection legislation. It is expected that this will still apply under GDPR, and may in fact become more common as the Data Protection Authorities look to dissuade others from failing to comply.

The fines described earlier in this article, albeit eye catching and interesting, are purely speculation. While the EU Commission has clearly defined what they *could* do, until the legislation actually goes into effect nobody knows with any certainty what they actually *will* do. We can only guess, and good arguments can be made on either side of the discussion, depending on whether or not you believe the real-world enforcement of the legislation will be as advertised. Regardless, there are other factors to consider.

Suspension of Data Flows

Article 58 outlines other powers of the Data Protection Authorities, and not all of them concern financial penalties. Such penalties may not grab the headlines, but they could easily be considered far more damaging to a company's bottom line. For example, it gives the authorities corrective powers such as instituting temporary and/or definitive bans on continued data processing; in other words, they can require an organisation to immediately halt all processing of the data in question. If the DPAs determine the non-compliance is severe enough and if it remains uncorrected, they could stop the organisation from using the data in any form. For some companies, that would be an irritating inconvenience; for other companies, it could mean the end of business operations all together.

The Hidden Costs of Non-Compliance

Putting aside punitive measures from DPAs, the other costs of a real-world breach can be staggering, and cases in the recent past should serve as a warning to us all. The Target Corporation, one of the biggest retailers in the United States, famously had tens of millions of credit card data records stolen by hackers in serious security breaches. The costs of simply repairing the breach - replacing the stolen cards and upgrading their terminals and security policies – were in the hundreds of millions of dollars. In the fourth quarter of that calendar year, company profits were down nearly 50% on the previous year; however, the resulting impact on both their brand and their corporate image is virtually incalculable.

The infamous Sony hack reportedly instigated by North Korea, serves as another stern warning, although the motivation for the breach itself was quite different. The direct financial impact to Sony after fines and legal settlements may have been smaller than the Target case; the reputational impact, however, is probably far more significant. It will be one of the landmark cases we think about when we consider the evolution of Data Protection requirements, made even worse by the fact that it isn't even the only major public breach they've suffered in the last decade (their PlayStation Network was taken offline by external sources back in 2011). Both occurrences were brought into the media spotlight, causing share prices to tumble and possibly causing irreparable harm to Sony's brand image.

Google and Facebook have also been involved in high profile cases in the EU in recent years. The details of those cases are not always clearly within a GDPR context, but nevertheless they concerned the way personal data was being processed and each case received significant professional and media scrutiny. That's not exactly the reason you want to find your company in the spotlight.

Summary

GDPR legislation has clearly defined the potential penalties for violations of the new regulations. While nobody can definitively predict the degree to which they will be enforced, it seems highly unlikely that first time offenders, companies facing minor breaches, or those with strong compliance measures who are doing their best to cooperate with authorities are going to be slapped with massive penalties under these circumstances. Data Protection Authorities may, however, choose to make examples of organisations who are repeatedly negligent or who demonstrate a general unwillingness to cooperate and comply, or of severe breaches of security, by imposing the headline-catching fines we discussed earlier.

Irrespective of official fines, nobody can afford the subsequent fallout that severe breaches bring about. A large multinational could suffer costs and reparations in the hundreds of millions, not to mention a huge impact on share prices. A smaller company offering data processing services could suffer a processing ban and loss of credibility with their customers; companies dealing directly with consumers could lose their business outright. Even non-profit organisations are at risk of losing donors or member participation.

We should be taking GDPR seriously – not because of the stiff fines and the regulatory requirements, but because protecting data is smart risk management and it makes good business sense to do so.

For more information about preparing for GDPR, contact Winterhawk Consulting:

infoeurope@winterhawkconsulting.com

http://www.winterhawkconsulting.com

LinkedIn **Winterhawk Consulting EMEA**

Twitter **@WH_Global**