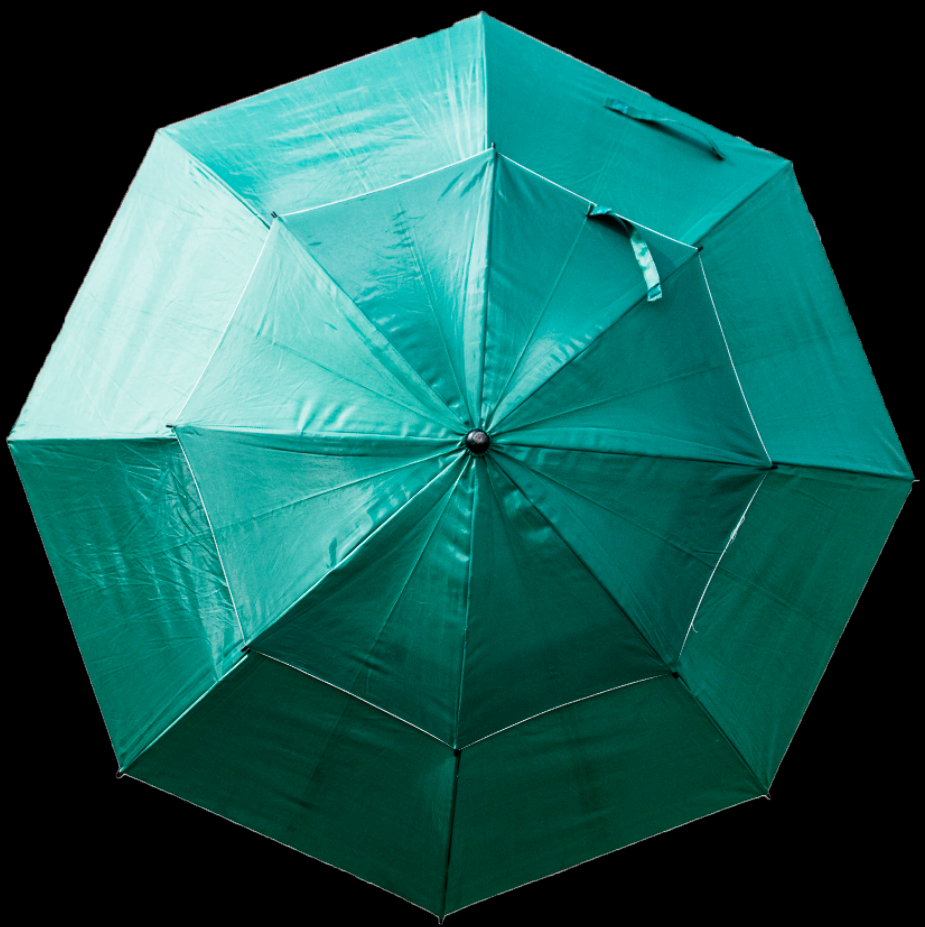
Deloitte.



Duty of care

What does it mean in the context of a data breach under GDPR?

February 2020

Contents

Introduction

Most people understand the term ‘duty of care’: The moral or legal obligation to ensure the safety and well-being of others. We complain loudly when duty of care is absent and shower praise when companies get it right, often by fixing a problem we have experienced, demonstrating that they care. In the business world, ‘duty of care’ is understood to be a key driver of customer trust (see Appendix 1), but what does it mean when your organisation is hit by a data breach?

We are now living in a world where the number of breaches and cyber-attacks, as well as the sophistication of cyber criminals, is increasing each year.

No amount of security can perfectly secure a system from intruders or remove the risk of errors by employees. Companies that have overlooked their duty of care to their customers after a data breach have seen significant and long-lasting reputational damage as well as financial penalties being imposed by the regulator.

This paper explores why ‘duty of care’ matters, the regulations surrounding it, and what constitutes a good, 'caring' response to a data breach.

Do companies need to exercise a 'duty of care' to their customers in a data breach situation?

Duty of care matters, and in the context of the General Data Protection Regulation (GDPR) it remains an important principle embodied within the regulation (Article 29). You should care about it not solely because of the loyalty and reputation it will create (or the customers you will surely lose if you do not look after them), but also because EU regulators are specifically guided to consider it when setting fines after a data breach.

Under Article 29 of Directive 95/46/EC (Data Protection Working Party), WP253 sets out the "Guidelines on the application and setting of administrative fines for the purposes of GDPR." These guidelines were subsequently endorsed for GDPR and provide us with some useful insight into how the regulators are being encouraged to think.

WP253 refers to an agreed "list of criteria the supervisory authorities are expected to use in the assessment both of whether a fine should be imposed and of the amount of the fine."

The third item in the list of the 11 assessment criteria (see Appendix 2) is as follows, and it relates directly to action taken after a breach to mitigate damage (i.e. to the exercising of duty of care):

"Any action taken by the controller or processor to mitigate the damage suffered by data subjects."

WP253 continues, providing very useful detail:

"The data controllers and processors have an obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, to carry out data protection impact assessments and mitigate risks arising from the processing of personal data to the rights and freedoms of the individuals."

"However, when a breach occurs and the data subject has suffered damage, the responsible party should do **whatever they can** do in order to reduce the consequences of the breach for the individual(s) concerned. Such responsible behaviour (or the lack of it) would be taken into account by the supervisory authority in their choice of corrective measure(s) as well as in the calculation of the sanction to be imposed in the specific case."

"Although aggravating and mitigating factors are particularly suited to fine-tune the amount of a fine to the particular circumstances of the case, their role in the choice of appropriate corrective measure should not be underestimated. In cases where the assessment based on other criteria leaves the supervisory authority in doubt about the appropriateness of an administrative fine, as a standalone corrective measure, or in combination with other measures in article 58, **such aggravating or attenuating circumstances may help to choose the appropriate measures by tipping the balance in favour of what proves more effective, proportionate and dissuasive in the given case. This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred."**

The two key considerations from the above guidelines are:

- **Rigour in breach prevention and security is important (as you would expect), but it is not the only factor:** When setting any fine, the supervisory authority will look at how well you have exercised your duty of care towards your customers after a breach, in addition to simply meeting the requirement to notify those deemed at high risk. So 'reducing the consequences' of a breach is important!
- **Tipping the scales:** In cases where a supervisory authority is in doubt about the appropriateness of a fine, the ability of an organisation to demonstrate it has exercised duty of care may tip the balance towards a more proportionate sanction. By virtue of their actions towards their data subjects after a breach, businesses can 'aggravate or attenuate' the fine.

"Whatever [you] can do to reduce the consequences" of a breach is a very broad statement. It is therefore valuable to consider exactly what is practically possible and reasonable for a data controller to do for their customers after a breach, and what 'good' looks like.

Supporting data subjects: Is 'good' enough?

Let's start with a view of what 'good' looks like in today's world.

Over and above fixing the vulnerabilities that allowed the breach to happen in the first place, practising proper 'duty of care' means supporting and protecting your customers. Guided by evidence of good practice from around the world, 'good' in customer support terms after a data breach is generally understood to include some or all the following activities: **Reset. Notify. Support. Monitor.**

Reset

- Immediate password reset action may reduce loss.
- Forcing a password reset is inconvenient for customers and businesses alike but can swiftly minimise the risk of fraud or loss.

Notify

- Let the impacted customers know they may be at risk of criminal targeting.
- Contact impacted customers "without undue delay" and in an appropriate manner (via email or letter, or the best channel to ensure they are properly alerted).
- Be as informative as possible by telling customers what happened, what data has been lost, what they should do to protect their identity, and what the data controller will do to support them.

Support

- Give customers someone to talk to about their concerns.
- Provide a helpline for impacted customers to call if they need help or advice from trained agents armed with a strong set of FAQs (many of which can be pre-prepared ahead of time) to help them understand what risks they may face and what action they should take.

Monitor

- Provide 12 months of access to individual monitoring and protection services to give warning if unusual activity is found suggesting a customer's data is being used inappropriately.
- Credit monitoring: Where available in the world (in Europe this is only in the UK), credit monitoring from organisations like Experian can be used to detect suspicious financial activity involving applications for bank accounts, loans, credit cards or credit checks. This can be important in breaches where financial data or sufficient data has been lost, such that there is risk of criminals attempting to make financial transactions.
- Dark Web monitoring: Used to search accessible areas of the Dark Web for an individual's data. The Dark Web is where stolen data is often advertised and sold. Importantly, Dark Web monitoring services can only search for data that is provided to them, and people who have just suffered a breach are often reticent to provide sensitive data to yet another third party.

"Failing to prepare is preparing to fail"

The list on the previous page shows what is available and has been used by many businesses to a greater or lesser degree in recent breach responses. Putting all of these actions in place swiftly requires advanced planning and the retained support of third party providers. However, many organisations fail to plan ahead and instead execute their plan on a knee-jerk basis, reliant on what the balance sheet or insurance cover might provide. Having a breach response plan in place that details the resources and mechanisms the business will use to support and protect customers — providing that 'duty of care' — needs careful preparation. It is likely that the initial costs involved could be offset by reduced future costs and fines in the event of a breach.

But is it actually 'good', or simply an accepted norm?

And is that norm still relevant? More to the point, with regulators shifting the burden of proof to organisations that have suffered a breach, and with duty of care one of the criteria that could tip the scales, what should reasonably be done after a breach? Just because consumers have come to expect a password reset, a letter or email, a call centre and the offer of monitoring, is that all that is practically possible? And can it be done faster to minimise any risk?

Looking more widely, what else can be done?

There's no doubt that 'Reset, Notify, Support, Monitor' provides a baseline of minimum criteria when appropriate, below which it would be hard to justify that an organisation has carried out its 'duty of care'. But technology and collaboration now provide businesses with additional tools that can be deployed. Taking proper responsibility would suggest that whilst helping people identify if their data is being used inappropriately is certainly of value, that value is diminished unless you can then help those individuals repair any damage caused.

So let's change perspective a little, and think about what customers might want after a breach
If it was your data, what would you expect? What would your 'minimum criteria for good' look like? How might regulators' view of 'good' begin to change in line with available services and/or consumer demand?

The following section outlines some of the other tools that data controllers could utilise in the event of a data breach. They are all available now, to all organisations who may wish to use them.

1. Repair

If people take up a data controller's offer of personal credit or Dark Web monitoring, and they find that someone is using their data illegally or inappropriately, what happens then? Some monitoring services may also provide advice on those next steps, but is that enough? Why, if your breach caused the problem, would you not support these individuals through the process of repairing their identity or recovering any lost funds?

2. Make it harder to submit loan or credit applications using stolen data

Many financial services organisations are members of CIFAS, an organisation set-up to help make it harder for criminals to take out loans or credit cards using stolen data. Instead of just offering people the chance to know when their data has been used illegally or inappropriately, why not make it harder to use in the first place? A two year subscription to CIFAS can be offered in the same way as credit or Dark Web monitoring.

What is CIFAS?

- CIFAS is a not-for-profit fraud prevention organisation that supports enhanced security in applications for bank accounts, loans or credit by maintaining a 'watch list' of individuals for whom additional checks must be made during any application process.
- This 'watch list' is populated in two main ways:
  - By individuals wanting to protect their identity, on a subscription basis.
  - By member organisations who share details of identities that may have been compromised.
- The 'watch list' is updated regularly and shared with all CIFAS member organisations.
- CIFAS members agree to put additional checks in place for any individuals on the 'watch list', making it harder for fraudulent applications to be completed for those people.

3. Looking after those whose data has not been breached

It might sound counter-intuitive, but by thinking about those customers whose data has not been breached, you could in fact benefit customers whose data has been lost.

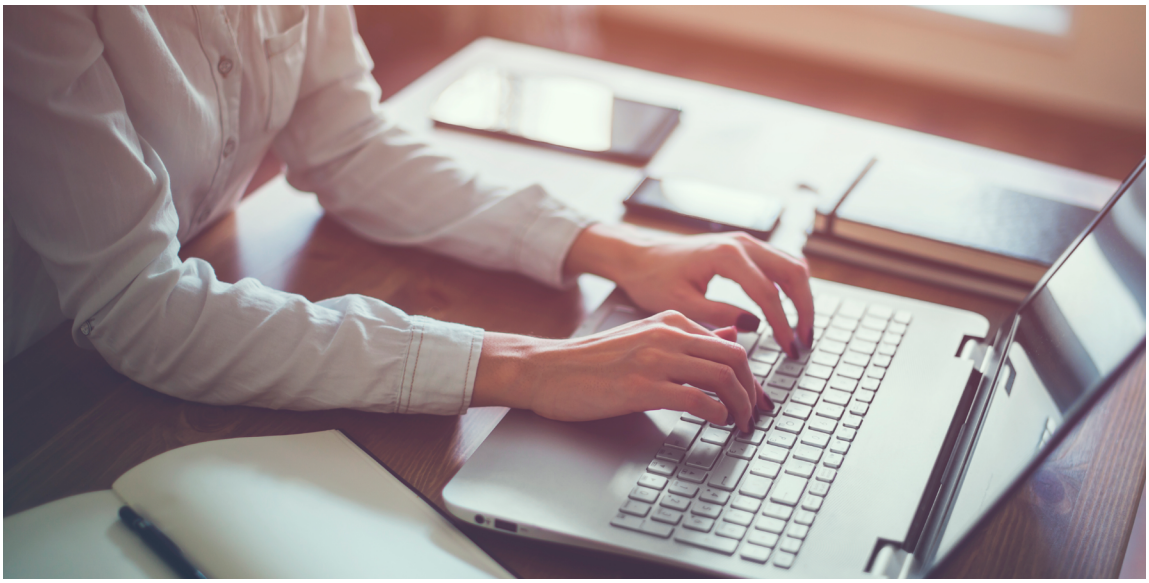
In the aftermath of a breach, when the media gets hold of the story, it is hard for people to know if they have been directly impacted or not. And if people don't know they will often call to check, increasing wait times and impacting service levels for customers who are a victim of the data loss and need your help.

Clear communication to all customers is therefore helpful after a breach (notwithstanding the challenge of finding out who is and is not impacted). If the story is trending on social media, organisations should manage consumer expectations and communicate clearly, so the picture can be better understood.

4. Business level Dark Web monitoring — by the data controller who has lost the data

Data is stolen for profit. Often, people who steal data are not the ones who use it for illegal purposes. Hackers sell their stolen wares to the highest bidder, or pass it on at the going rate, and they do this via forums and markets on the Dark Web. Cost-effective monitoring services exist to allow companies, with a legitimate interest, to constantly search the Dark Web for evidence of any of the data they hold on all of their customers, without a 12-month expiry date, and across open and closed forums.

One-way hashing (encryption) tools allow this to be done securely, without further risk to consumer data privacy (see box overleaf). With the take-up of individual credit or Dark Web monitoring services being very variable (typically between 5% and 10% of impacted consumers sign up to the service they are offered), post-breach Dark Web monitoring by the controller can provide an additional level of protection for all data subjects.



What is a 'one-way hash'?
Simply put, this is the process of encrypting a piece of data in such a way that the encryption process cannot be reversed (I can produce 'XYZ' from 'ABC', but I cannot reverse the process and get back to 'ABC' from 'XYZ'). Importantly, the one-way hashing process produces unique outputs from unique inputs. So, if 'XYZ' is indeed the result of putting 'ABC' through a one-way hash, 'XYZ' can only ever be produced if the input is 'ABC'.

How can companies use one-way hashing to search securely for consumer data on the Dark Web, without further risk to consumer data privacy (i.e. without providing a copy of that data to the organisation or platform that will undertake the searching)?

The process works as follows:

- Within the secure boundaries (firewalls) of an organisation, a one-way hash is run that encrypts the data to be searched for. Let's use a simple example and assume we hash 'mark_whitehead@wysiwyg.com' and that the output is '888ydt£32'.
- The hashed data (888ydt£32) and the one-way hash tool is given to the company running the Dark Web search. Because the encryption is one-way, the search company (or any organisation that might compromise their systems) will never be able to discover the original data, even though they have the one-way hash tool and the output data string.
- The search organisation uses its tools and techniques, both automated and/or manual, to search the Dark Web for data. Modern processing capabilities effectively allow the entire 'open' Dark Web to be searched. 'Closed' Dark Web forums require manual search capabilities.
- The search organisation then puts the data it has found into the one-way hash tool.
- If one of the results from the one-way hash is '888ydt£32' then the search organisation knows that 'mark_whitehead@wysiwyg.com' is present on the Dark Web, and appropriate action can then be taken.

5. Responding and supporting at greater speed

It is an obvious statement, but the faster you are able to respond after a breach, the sooner action can be taken to protect consumers. This is emphatically not a call to react with haste or on incomplete findings (there are enough well-publicised cases to highlight the drawbacks of such an approach), but a restatement of an age-old adage that preparation in advance of an incident increases the chance of dealing with that incident in the most effective manner.

Assess, plan, learn, and practice. Then repeat.

Data breaches are a unique and highly dynamic type of crisis, with a huge array of stakeholders to be supported through the journey. If you are not used to dealing with breaches, and all of the many factors that impact your 'breach readiness', then the chances are you will deal with them poorly, and your customers will suffer accordingly.

Make sure your strategy and plans are in place and routinely tested. Bringing in third parties to support the readiness and testing processes will help reduce assumptions, provide new viewpoints and increase robustness. It's interesting to note that in the case of an airline's recent data breach, the regulator mandated remedial action that includes ongoing reviews by specialist third parties to provide independent validation of security measures.

At a high level, the key areas that need to be considered in your breach readiness planning are:

- Incident management
- Cyber and digital forensics
- Customer notification and support
- Legal, insurance and regulatory
- Communication and reputation management

Reaction time can also be reduced by implementing a number of proactive tools that monitor for early warnings of a breach

These range from system monitoring tools and simple social media and internet monitoring, to the use of 'breach markers' in Dark Web monitoring. Breach markers are unique data sets created by you for specific databases across your system. If they appear on the Dark Web then you will know that you have been breached, and from which system across your network the breach occurred. This technique, which is much less expensive and intensive than continuously trawling the Dark Web for all of your data, can also help to reduce the significant number of false positives that are found when undertaking Dark Web searches for common data elements like names, usernames and email addresses, which are often already present on the Dark Web, harvested by other means and from other organisations.

Conclusion

All businesses have a duty of care to their customers, and it probably drives much of what your organisation does on a day-to-day basis. It will certainly drive your brand and reputation.

Duty of care is valued most by your customers when you are acting to help, support and protect them, often when something goes wrong. And if you fail to measure up in times of crisis, customers are becoming more and more likely to vote with their feet (or, in today's digital world, with the click of a button).

When you do suffer a breach, not only will your brand, reputation and customer retention suffer as a result, but if you cannot demonstrate that you have done all you can for your customers, then your balance sheet might take a greater hit from the regulator (see Appendix 2). Recent fines by the Information Commissioner's Office (ICO) show that GDPR has sharp teeth, and the assessment criteria that supervisory authorities use when setting the level of fine are there for all to see in the regulations themselves.

It is not being suggested that the 'duty of care' criteria is the only factor that organisations should focus on. However, out of all eleven criteria that regulators are asked to consider when assessing and setting fines, it is the most relevant for your customers, the lifeblood of your business.

If, as the ICO stated in 2018, "the risk in a personal data breach is to the data subjects", then once a breach has happened, and your customers are having to deal with their new reality, shouldn't you be doing all you can to mitigate their risks? And if the prospect of ICO fines isn't enough to change behaviours, then perhaps the spectre of class action — driven by Lloyd vs Google and Justice Warby's recent ruling — might go some way to persuading organisations that the reputational and financial risks from a data breach have never been greater.

Appendix 1 – Trust, reputation and duty of care

Duty of care is a key facet of trust, which is critical to brand and reputation

What is trust?
Simply put, trust in an organisation means you have confidence that they will look after your best interests.

Why is trust important?
Trust is the basis for long-term, mutually beneficial, sustainable relationships.

What can organisations do to build trust?

- Trust is based on three key components: what you say, what you do, and how you perform.
- Organisations build their narrative through behaviours and actions, with PR and corporate affairs providing momentum through content and news.
- Trust is continually earnt, requiring ongoing commitment and action to ensure it remains present in the minds of customers.

The 2019 Edelman Trust Barometer provides insightful information about trust in today's environment, highlighting its importance for reputation and its critical dependency on duty of care.

Key points from the 2019 Edelman Trust Barometer:

- People are buying based on trust, across markets, ages and incomes:
  - Consumers rank trust with product, brand and company attributes as an essential buying consideration.
  - Consumers want to trust brands to do what is right with their product, for customers and for society.
  - Consumers expect brands to keep their promises by taking action that makes a real difference; trusted brands act on their words.
- When brands build trust, people will buy, stay loyal (buy again), advocate the brand to others, and defend the brand if it is challenged.
- "A good reputation may get me to try a product, but unless I come to trust the company behind the product, I will soon stop buying it."

Appendix 2 – Regulatory criteria for assessing and setting fines

What are the criteria supervisory authorities use in setting fines?
As noted in the conclusion, "any action taken by the controller or processor to mitigate the damage suffered by data subjects" is just one of the 11 criteria that regulators are asked to consider when assessing and setting fines.

The full list of criteria is:

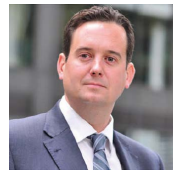
1. The nature, gravity and duration of the infringement
2. The intentional or negligent character of the infringement
3. Any action taken by the controller or processor to mitigate the damage suffered by data subjects
4. The degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32
5. Any relevant previous infringements by the controller or processor
6. The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement
7. The categories of the personal data affected by the infringement
8. The manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement
9. Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures
10. Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42
11. Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

These criteria are provided to the supervisory authorities to act as guides against maximum fine levels of 2% or 4% of global revenue for organisations that fall foul of GDPR. If we assume that all 11 factors have an equal weighting (highly unlikely, but no weighting guidance is provided), then what is 1/11th of 2% or 4% of your global revenue? Against that metric, what amount of risk capital would you invest to offset the risk of a maximum fine for each of the 11 factors?

Source: Article 29 of Directive 95/46/EC (Data Protection Working Party), WP253: "Guidelines on the application and setting of administrative fines for the purposes of GDPR."

Contact us

Mark Whitehead
Director
Risk Advisory
+44 (0) 20 7303 0698
marwhitehead@deloitte.co.uk



Hugo Morris
Partner
Risk Advisory
+44 (0) 20 7303 5985
hmorris@deloitte.co.uk

Deloitte.