Ten top tips for managing data breaches

Jonathan Armstrong of Cordery shares his experience on how to prepare for, and manage a data breach, as well as benefit from lessons learnt.

Dealing with a security breach, even in these unusual times, is often the toughest aspect of a data protection professional's job. As we are heading toward the second anniversary of GDPR, we thought it might be interesting to share some of the lessons that we have learned from handling security breaches across the EU. We have also done some work looking at public cases and we have included examples from around the EU to illustrate the points we are making. In some cases, we have used pre-GDPR cases where we think they are instructive. We have boiled all of this down to ten top tips for handling a data breach. Most of this is common sense but you can use these tips as a checklist to make sure your processes are robust.

1. Have a Plan

It is a simple fact of life that data breaches are inevitable. For most organisations it is a "when" not "if". Even the best organisations will have breaches. Once you have accepted this mind-set it is easier to understand that you must prepare. Many of the issues that we see are where clients either do not have a plan, or have a plan that is so detailed that nobody reads it and as a result they just ignore it when there is a breach. A really technical 45-page plan that you ask employees to read is as good as having no plan at all. What most organisations will actually need is two plans:

A. A simple plan for all of their employees to follow that tells them how to recognise a breach and what to do when they see one. We often liken this to the type of notice that you get on the back of a hotel door telling you how to raise the alarm and how to get out of the building. Try and keep it just as simple with clear guidance. Just as in a fire there is another parallel with these signs – we used to tell people which fire extinguisher to use for which type of fire and how to work out the source of the fire. We do not do that any longer – we just tell people to raise the alarm. It is the same with data breaches. One of the real causes for delay is that people sometimes think they have got to report a problem and a solution. They don't! Your obligation is to report a problem, and in most cases, it will be down to the team of experts to work out a solution (or at least mitigation). This might be where the second plan comes in.

B. A more detailed plan that the data breach team use as their guide. This team also needs to rehearse. We have had real success with our Data Breach Academies which involve walking data breach teams through as realistic a scenario as we can. It works a little bit like muscle memory. Once the team know each other, they know how they will work better together. Invest the time to make sure you can respond quickly.

2. Know your Data and your Third Parties

There are many issues in modern day organisations partly because we live in a disaggregated world and many organisations outsource tasks that even five years ago would have been regarded as routine. Many organisations do not know exactly where their data is and we have been involved in breaches where a third party has told the data protection team about a data breach and the data protection team did not even know that this vendor was being used. You will need to do proper due diligence on providers and contracts.

This goes for acquisitions as well. The Marriott data breach case for example tells us of the need to do proper due diligence if you are acquiring an organisation to make sure that there is not an issue hidden away. For many organisations this will be a board level responsibility. For example, see the words of Elizabeth Denham in the Equifax breach: "Multinational data companies like Equifax must understand what personal data they hold and take robust steps to protect it. Their boards need to ensure that internal controls and systems work effectively to meet legal requirements and customers' expectations."

3. Assemble your Team

As we said it is important that you have an established data breach team and that they get used to working together. You can co-opt people onto the team but make sure you have all the right skills there – not only people who are good technically but people who are also good at explaining technical issues. You will also need to consider somebody responsible for PR and if you are a listed entity, somebody who is keeping an eye on your responsibility to stock exchanges and investors given the possible impact on your share price.

The *Morrisons*' case (even in its toned-down Supreme Court incarnation, p.24) also tells us that you will need to do due diligence on that team – there is going to be a lot of sensitive data passing through the data breach team so they need to be people that you can trust completely. As we have said before, rehearse, and if you are a multinational organisation, pay particular attention to culture.

4. DPIA Everything

It is our experience that where there is a breach with a process that has been through a data protection impact assessment, you will be in a much better place to react quickly. There is also anecdotal evidence that you are much less likely to suffer a data breach with a process that has been through a proper DPIA. It is important to make process owners responsible for putting the DPIA together. The DPO or legal

department should not bear the responsibility of doing all of the DPIAs. The proper risk owner should own the risk with the DPO and legal in most cases as the second line of defence.

5. Do DSARs well

Data Subject Access Requests are often a sign of some other pain in the business. Whilst we know that some are made on a scattergun basis – and the rise of third party apps has not helped – sometimes people make a data subject request because they think that there has been a security episode that the organisation is just not talking about. If you have the right systems and processes in place you can use the receipt of DSARs as an advanced early warning system. Make sure that your processes are robust and that the team handling DSARs know to raise the alarm with the data breach team if they have a suspicion that something might be going on.

6. Respect the Time

Many of the breaches we see are not reported in time. Part of the reason for that is the thinking within the business; they believe that they have to report a problem and find the solution at the same time. In part it is a sort of perennial optimism that the breach is not as bad as it seems. Unfortunately it often is. As an example, you could look at Talk Talk's appeal to the First Tier Tribunal in 2016.

You can't hide behind uncertainty – if in doubt be ready to report within the 72-hour period. You don't need all of the answers to make a report and you can provide the information required by GDPR Art. 33 in stages (see GDPR Art. 33(4)).

And remember that the 1&1 case in Germany[1] confirms to us that there doesn't have to be actual harm for a breach to be reportable.

7. Remediate then Report

In our experience, DPAs will give credit when an organisation shows that it has learned lessons. We have worked hard to put together lists of mitigating or remedial factors for different breaches based on previous regulatory findings. It is a good idea to go through a list like this before you submit the report (if you have time) and decide what you are prepared to commit to there and then. There might be some simple measures that you can agree quickly – like issuing padlocks to people who carry hard copy data; installing new software on laptops or organising enhanced training for the team responsible for a breach. If you can commit to doing those things when you report the breach then regulatory intervention is less likely, and if a regulator does still sanction you, the penalty is likely to be less severe. Conversely if you are cavalier about victims or you try and impose new contractual terms on them in exchange for information (like in one breach) the consequences are likely to be worse.

> You should learn from every incident – whether reported or not.

8. Don't diss the DPA

Unfortunately we have seen a number of cases (for example Cambridge Analytica[2] and Doorstep Dispensaree[3]) where organisations have shown disrespect to the regulator. That is never a good idea. You might not agree with the regulator but you need to show them respect. That is not the same as accepting their findings – many data breach penalties will be subject to appeal – but it is wise to remain professional both to the regulator's face and in the press.

We are increasingly seeing that regulators are becoming more technologically astute when looking at breaches – see for example the Monetary Penalty Notices in DSG/Carphone Warehouse[4] and Cathay Pacific[5] so it will not be easy to pull the wool over their eyes. Be aware of the fact that regulators can and will ask you to commit to a host of remedial measure in addition to a monetary penalty – see for example the Doorstep Dispensaree case in the UK or the TIM case in Italy[6] where the Enforcement Notice contained 20 different remedial measures.

9. Keep Logs

It is important that you keep a proper log of data breaches whether or not they were reported. There is a clear trend of individuals making Subject Access Requests when they suspect there has been a breach, and you might need to show your data breach log to a DPA if they ask for it. In these times of increasing civil action, that is likely to be on the list for a claimant's solicitor as well.

10. Debrief and Learn

The simple fact with a data breach, as with any other form of crisis in an organisation, is that it is never over until it's over. We sometimes see repeated breaches with the same vulnerability being exploited over and over again – this has been a particular hallmark of Office 365 attacks. It is important that you debrief properly. Look regularly at your remediation plan and try and make sure it does not happen again.

You should learn from every incident – whether reported or not – and it is often a good idea to involve the whole of the data breach response team in that debrief so that you can learn from past experience.

AUTHOR

Jonathan Armstrong is a Partner at Cordery.
Email:
jonathan.armstrong@corderycompliance.com

REFERENCES

1 bit.ly/gergdpr11
2 bit.ly/cambridgesar
3 bit.ly/gdprdoor
4 bit.ly/carphonebr
5 bit.ly/cathayico
6 bit.ly/gdprtim

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Returning to work: Covid-19 and the UK data protection perspective

Nicola Fulford and **Hannah Jackson** of Hogan Lovells report on the data protection aspects organisations should consider with regard to coronavirus testing and processing of health data.

Individually, many of us use data to track our progress – from fitness gains to home energy consumption; we watch information about our lives and use it to inform our activities. On a larger scale, numerous organisations have made significant investments in data analytics capabilities, and at a state level, a vast quantity of information about populations is used to direct public policy. It is not unreasonable,

Continued on p.3

Winner of the ICO's Data Practitioner Award: Barry Moult

The regulator's annual award recognises a long career in NHS Information Governance and innovative thinking. **Laura Linkomies** talked to Barry Moult about his work.

The 2020 ICO Practitioner Award for Excellence in Data Protection was awarded to Barry Moult, Information Governance and Privacy Consultant, and former Head of Information Governance and Health Records at the Colchester Hospital University NHS Foundation Trust. Recently retired from his role at Colchester, which he held from 2014 to 2018, Barry is now utilising his decades-

Continued on p.5

Issue 109 **MAY 2020**

UNITED KINGDOM
report

ISSUE NO 109 **MAY 2020**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Nicola Fulford and Hannah Jackson
Hogan Lovells

Josephine Jay and Christopher Foo
Wilson Sonsini Goodrich & Rosati

Victoria Hordern
Bates Wells

Emma Erskine-Fox and Gareth Oldale
TLT

Rebecca Cousin and Cindy Knott
Slaughter & May

Jonathan Armstrong
Cordery

David Barnard-Wills
Trilateral Research

Camilla Ravazzolo
UK Market Research Society

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

Stay alert to Covid-19 data protection issues

There is unfortunately still much uncertainty about when we are back to "normal" life in the UK. The 'new normal' will most definitely include new rules and procedures at the workplace when offices start to reopen. Read on p.1 our correspondent's analysis of the data protection implications at the workplace.

We recently carried out a survey to find out about the challenges that DPOs encounter due to the pandemic. There are implications across the board: for remote working, data security, processing employee data etc. Read on p.12 how organisations are tackling these issues. Normal compliance work, for example processing Subject Access Requests has not gone away – in fact some organisations are seeing an influx of requests relating to furloughing and employee health records (p.9). While employers may ask staff whether they have Coronavirus symptoms, they should not ask unrelated questions, for example about underlying medical conditions, or symptoms not associated with Covid-19. The NHSX contact tracing app may help to control the virus but has privacy implications (p.8).

If home working and social distancing continues for the rest of the year for many, it will undoubtedly create a new work culture in some organisations. DPOs may become more reliant on webinars and online team meetings to exchange information. *Privacy Laws & Business* will soon launch a value-added way for you to connect with our expert consultants to address your specific questions during an initial half-an-hour consultation.

In this issue, to keep you well-informed, we bring you updates on AI legislative developments (p.16), how to choose your legal basis for adtech (p.22), the implications of the Supreme Court's Morrisons vicarious liability decision (p.24), top tips on managing data breaches (p.27), data protection issues for SMEs (p.20), DP issues in scientific research (p.29) and an interview with the ICO award winner (p.1).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

> *PL&B UK Report* offers excellent guidance for Information Management professionals on the latest changes in data regulation, as well as useful advice on improving data security and protecting privacy.
>
> **Simon Baker, Nursing and Midwifery Council**

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 33rd year. Comprehensive global news, currently on 165+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.