

## Life With GDPR: Episode 33 - Lessons Learned in Year 1 of GDPR, Part 3

**Date :** September 19, 2019

<https://youtu.be/etWf2BS3qAs>

In this podcast, Cordery Partner Jonathan Armstrong and Compliance Evangelist Tom Fox use the framework of GDPR to discuss a wide range of issues relating to these topics. They consider what the US compliance and InfoSec security expert needs to know about what is happening in the UK, Europe and beyond.

In this episode, we conclude our three-part series of some of the key lessons learned from the first year of GDPR. Some of the issues and highlights are:

### ***Remediate then report.***

The remediation of an issue before reporting can be the key issue for regulators on whether they take the matter further with the imposition of a fine. It is important to show that you have learned lessons and applied them to the facts of your data breach. Don't try and cheat the victims by imposing new contractual terms such as Equifax did in its recent settlement. Think of the simple way for a data breach to occur, for example a briefcase left on the Tube.

### ***Don't Disrespect the DPA.***

Why would a company take on the regulator? You must respect the regulator even if you disagree with them. You can make a bad situation worse by attacking the regulators. This does not mean you cannot forcefully argue your position or zealously represent your client but calling regulators idiots in public filings will not help your position or your case.

### ***Keep logs.***

This is important in case you need to revisit a decision later. Regulators can ask to see these logs at any time, not simply during an investigation or enforcement action. A compliance officer should be involved in the maintenance of the log system. *Document, Document, Document.* Unannounced inspections are beginning to occur.

### ***Debrief and Learn.***

Revisit the facts to see what lessons are to be learned. Continuous improvement. Even on a journey of 1000 miles, it is important to look back. Once again if you make a change due to a breach or other event, document what you have done so you can show the regulators.

Organisations need to make sure that they do all that they can to stop data breaches. They also need to ensure that they can react to data breaches quickly when they do happen. Cordery's Breach Navigator can help organisations respond to a breach. There are more details here: <https://www.corderycompliance.com/solutions/breach-navigator/>.

For more information please contact Jonathan Armstrong or André Bywater who are London-based lawyers with Cordery where their focus is on compliance issues.

[Jonathan Armstrong](#)

Office: +44 (0)207 075 1784

[jonathan.armstrong@corderycompliance.com](mailto:jonathan.armstrong@corderycompliance.com)



[Andre Bywater](#)

Office: +44 (0)207 075 1785

[andre.bywater@cordeycompliance.com](mailto:andre.bywater@cordeycompliance.com)

