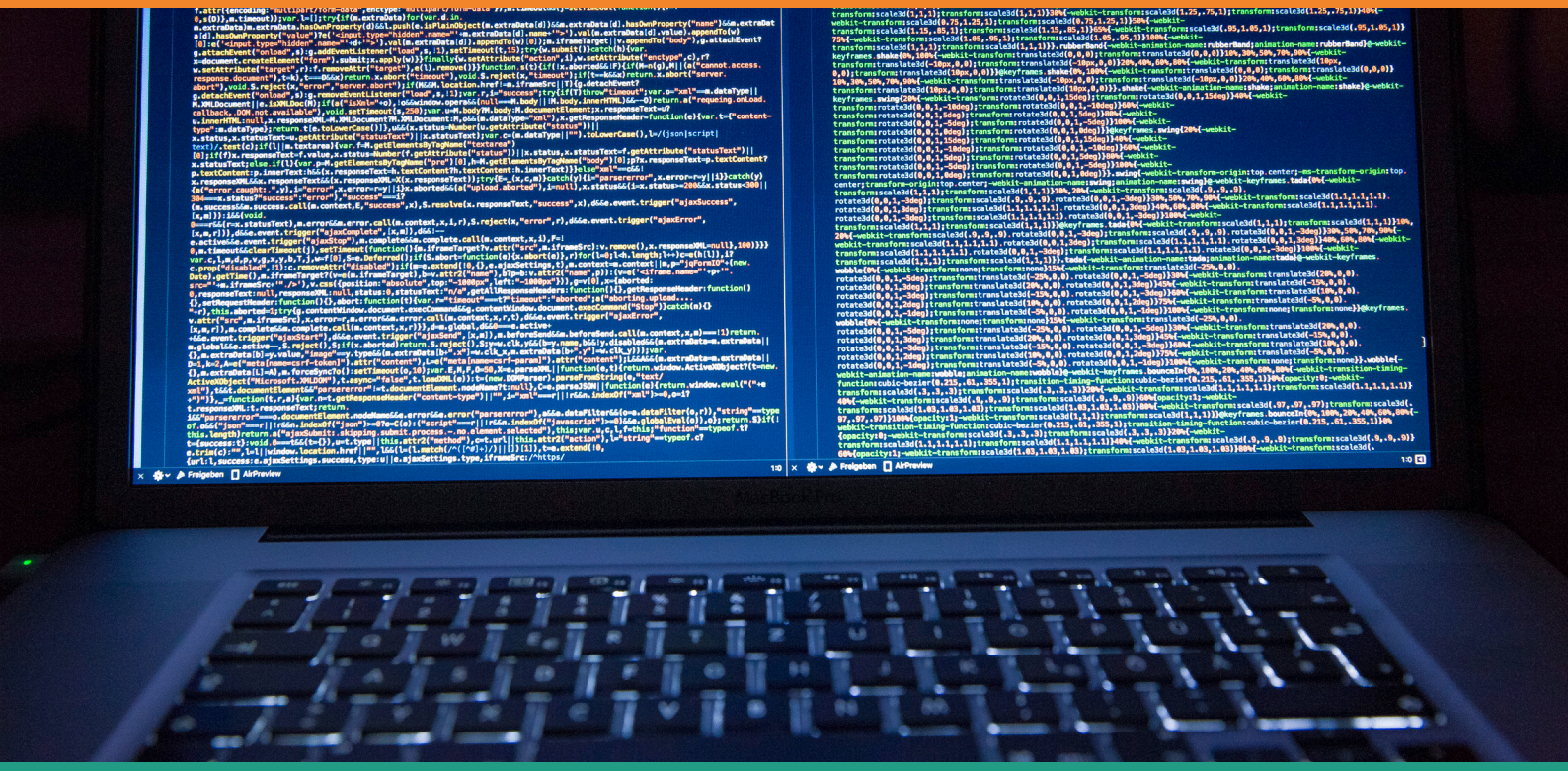
Metis Insights for Consultants: How new data privacy rules will affect you and your clients



For businesses across the EU, 2018 sees the biggest change to privacy and data protection legislation in over 20 years. Bringing regulations in line with the modern digital environment, the widespread adoption of e-commerce and increasing concerns over online security, the General Data Protection Regulation (GDPR) will transform the landscape of data collection and its usage. Companies across all 27 EU member states that process personal data are being urged to consider their ability to comply with new standards, and to take the appropriate measures in preparation of the changes ahead. Not even Brexit will offer respite, as it is likely that the new regulations will be adopted into UK law as part of the government's planned Great Repeal Bill.

Differences that consultancies can expect to see range from a large increase in fines for data breaches (up to 4% of annual global turnover), to the potential need to appoint a Data Protection Officer. Overall, companies will now be expected to adhere to stricter rules surrounding the capture, usage and protection of personal data, whether that be of employees or clients, and may be required to prove their compliance to external authorities as and when requested.

As James Leaton Gray, former Head of Privacy at the BBC, explains, "The new level of expected accountability means that you're not just having to obey the law, you're going to have to be able to demonstrate how you've obeyed the law. Regulatory authorities will now have the power to request paperwork and evidence of your procedures at any time, so we've got to get used to the idea that as well as doing it, we also have to note down that we've done it."

Transparency towards client privacy in consultancies

Achieving this level of transparency will be key in not only meeting new legal requirements, but in building client and employee trust. As employers, consultancies are automatically privy to personal and financial information about the individuals who work for them, as well as ongoing employment data such as assessments and performance reviews. They also hold sensitive company and commercial data belonging to clients, such as business information, customer research, operation data analysis and even insights into the working attitudes of clients and their staff.

The responsibilities consultancies hold towards both staff and clients will be increased under GDPR. "You're likely to almost automatically have sensitive personal data about your employees and clients, so you're going to have to treat that much more carefully under the legislation." The obligations of a consultancy will be to ensure that data is collected with explicit consent, rather than implied, to allow clients to see the data you hold on them when requested, and to exercise their right to be forgotten and to have this data erased.

With this in mind, the way that all businesses approach the customer experience will need to be considered. James continues, "There are going to be quite a lot of changes in the areas where you are interacting with customers, and quite a lot of user journeys will need to change. There'll be a lot more information that will need to be put onto websites in a manner which isn't too intrusive, yet fulfils the law."

The ways in which consultancy firms communicate these privacy policies will come under the scrutiny of the new legislation; "How do we make sure that we are transparent and tell people enough about what we're going to do with their data without boring them? They're so fed up of getting messages that it actually turns them away from us. I think there's going to be a real challenge to be open enough to fulfil the legislation, but also do it in a way which is engaging with the audience."

As client awareness of GDPR grows, the pressure on firms to meet customer expectations may increase. While many may not initially be familiar with the new regulations and what they mean to them, James envisages this changing over time, with some clients taking the opportunity to enforce their expanded rights.

"There are activists out there who feel very strongly about this and they're likely to be using their new rights both for themselves and on behalf of others to try and ensure that companies take this new legislation seriously. I think you're also going to get increasing use by the wider public when they realise that they do actually have these rights. At the moment there are Subject Access Rights, whereby we can all go to a company and ask to see the data they hold on us, but the company can ask for a £10 fee, which is a disincentive. That £10 charge disappears under the new regulation, so you could see an increase in uptake."

Privacy at the heart of your consultancy

As we all adapt to an internet-fuelled economy, these new regulations will not only affect the way that businesses operate, but the importance we place upon online safety and the privacy of all our professional and commercial interactions. James feels that companies and the public are overdue for improved levels of security, saying "With the increased pace of digital services as we move into an online world, regulation does need to follow. We expect certain standards and we expect to be protected in certain ways. This piece of legislation provides a level of assurance to the average person that if they go online they're going to be protected and that all companies online have to take their responsibilities that little bit more seriously."

In taking these responsibilities more seriously, companies will have to incorporate privacy considerations into their entire infrastructure, embedding data privacy into the business ethos and all of its operations, rather than as a separate HR task. "In the future, privacy isn't going to be something that's sitting off somewhere in legal or compliance as a form that's ticked once year.
There is a principle which has to be followed called "privacy by default", which requires brands to think about all of their systems as being privacy friendly from the start. You'll also have to adopt "privacy by design", which actually bakes privacy into the development process of a product. So in future, operations teams and designs teams are all going to have to be brought into compliance.
It'll have to be embedded into the company, and that is going to be a very big change. It's as much a philosophy challenge as it is a practical challenge"

James believes that for some companies, this will mean an overhaul to their entire working culture; "There are a large number of businesses that are a little shy about telling their staff, customers and clients what they do with their data, and there are some business models that are set up specifically around the assumption that they can do anything they like with that data. That is going to have to change under the new regulations."

Building privacy into all stages of company ethos and product development stages will affect the advice that consultancies need to be passing on to their clients. As experts in their field, consultants will need to understand the principles of privacy by default and privacy by design in order to communicate these needs to clients. Consultants who don't advise clients on these aspects of working privacy into the core of working practices and new products risk reputational damage should their clients fall foul of the GDPR due to lack of the correct professional information.

Preparing your consultancy for GDPR

One thing is clear; in order to incorporate privacy considerations into all of their working practices, consultancies need to be planning, updating and implementing their privacy strategies before GDPR is enforced. James reiterates the importance of planning ahead:

"A surprising number of businesses aren't aware of this change or are ignoring it, hoping it will either go away or won't be as bad as it sounds. You have to have measures in place to track things, undertake privacy impact assessments, implement data protection by default... are you going to need a Data Protection Officer? You need to be doing a gap analysis against your present capability and then measuring that against where you need to be, and start moving towards closing those gaps."

For many consultancies, awaiting the results of the EU referendum was enough to put GDPR preparations on the back burner. Whilst it's likely that the UK won't fall directly under the GDPR, the UK government may adopt it alongside other EU legislation as part of the planned Great Repeal Bill. However, regardless of how the UK government decides to modify the legislation in the future, the GDPR (including its penalties) will still affect any UK business offering any kind of service to the EU market, and governs the collection of data from anyone within the EU, regardless of whether you are situated within the EU itself or not. So for consultants who work with EU clients, or whose clients have any dealings with Europe, complying with GDPR themselves and having a professional working knowledge of how clients should implement it are still absolutely essential.

Failure to comply

Companies who remain unprepared could see themselves at the sharp end of GDPR. Breaches will now need to be reported to authorities within a 72-hour deadline, a time frame that businesses may not yet be equipped for.

"A data breach is the loss (and it could be accidental destruction as well as hacking) of data that has been collected. Or a breach is data being used for the wrong purpose, whether you didn't have the right to use it for that purpose or somebody's stolen your database. You're going to have to inform the regulator within 72 hours, telling them how much data was involved, what the data was and what were you using it for."

Even if you already have a data breach system in place, something to try and inform management and then potentially inform regulators of lost data, it's highly unlikely it's set up to work within 72 hours.

Failure to comply with GDPR can bring monetary penalties, but it isn't just financial loss that threatens the disorganised. The increased profile surrounding data privacy issues means that poor compliance could also mean adverse publicity and loss of reputation. James explains that businesses need to be well rehearsed should the worst occur;

"It's been building over the past few years, as people become aware of internet identity theft, so have the press. Losing a database might have seemed a very technical thing ten years ago and not particularly newsworthy, but now it might well get you on the front page. Individuals such as CEOs who are seen not to perform well in those circumstances are being really crucified by the press because they weren't able to provide good enough answers. They have to talk to the regulators and this has an impact on their public profiles, so their customers see them as being not very effective guardians of that data."

There will be much larger fines, and although these could potentially be huge figures, they can actually be dwarfed by some of the other effects on the company – damages to reputation, and potentially the share price, customer retention and certainly new customer recruitment.

As James concludes, "Start thinking about data breaches now - don't think it's never going to happen to me, plan for when it does."

The Metis Action Guide:

In order to be correctly prepared for the enforcement of GDPR, your consultancy needs to be taking action **now**. Here's the five step action guide from Metis to ensure that your consultancy business isn't left behind or fined.

1. If you haven't already done so, register your firm with the Information Commissioners' Office at https://ico.org.uk/. This is the UK's independent authority upholding information rights and data privacy.

2. Start with your own team. Ask yourself whether data you hold about your consultancy staff is secure, and how it can be better protected. This might include personal histories and financial information, internal assessments and competency reviews.

3. Review any client data you hold. How are you storing personal data, and have you agreed these standards with the client? You will need to have communication strategies in place to inform clients how their data is held and used, processes for obtaining new client data, and to be prepared for the right of clients to see the details you have on them.

4. Check the impact on any recent, current or forthcoming projects. Will the new regulations affect the design of services, the level of security required or the budget for the projects?

5. Check whether your clients are aware of the new regulations, as you will be required to explain the changes to them and to help implement new practices to prevent them being in breach. Is there an opportunity for you to help your clients alter existing methods, and incorporate privacy requirements into new services and operations?

James Leaton Gray

At **The Privacy Practice** James provides bespoke consultancy services in Data Protection and Privacy for a variety of companies and sectors. These range from financial services and retail, through to law and digital services. James specialises in privacy implementation advice, GDPR readiness reviews and strategic data policy guidance. He also designs integrated privacy programmes, for example for the BBC's personalisation and big data capability. As well as running the Privacy Practice he is a Consulting Director at Deloitte and the lead privacy consultant at Kemp Little Consulting.

For over 10 years he headed the BBC's Information Policy and Compliance Department overseeing the corporation's systems for compliance with the Data Protection and Freedom of Information Acts. Before that he worked on a variety of policy and management roles in the BBC following a career in current affairs and political programmes production.

About Metis

The minds that make Metis tick

Metis is built by a small team of entrepreneurs who have founded, grown and sold companies like yours.

We know what it's like to manage all stages - from when there are just two of you, to when you're dealing with hundreds of people in multiple teams.

Metis is the distillation of the lessons we have learned along the way.

Our mission is to make businesses like yours more successful.
We'd love to show you how we can help.

metis

getmetis.com
+44 (0) 20 3475 5165