The GDPR Myths vs Reality

Written by Paul Mather, EU-GDPR-P, EU-GDPR-F

About the Author

Paul Mather is a registered GDPR Practitioner and a Director of Operations with Dillistone Group PLC, serving thousands of corporate and recruitment clients worldwide.

Don't get caught out by the hype

Before you think this is "just another GDPR whitepaper", let's just think about that statement. For once, public momentum has outpaced the legal profession, government and, in this instance, national supervisory authorities. More information about the GDPR, what it means and what you need to do to get compliant has come from independent sources than "official" ones, and by a considerable margin. It now seems likely that the GDPR will drive the largest changes ever, for organisations in how they deal with personal Information, yet a year ago few had heard of it. A good proportion of businesses, I'm pleased to say, do seem to be taking this seriously. That's a good thing for all of us, as we all have personal data that is currently out of our control.

For those of us that work in and around the recruitment sphere, data protection (and in particular its legislation), as we'll discuss later, has come as a bit of a surprise for many. By this, I mean that a lot of boards have been ignorant of their requirements under the old data protection legislation, data subjects have been ignorant of their rights and supervisory authorities haven't been aware of the scope of data held by many agencies and the lawfulness of doing so. The GDPR has forced these issues to the fore and once again, positive changes are happening in all these aspects.

The biggest drawback which comes from the (deliberate & necessary) vagueness of some of the definitions in the GDPR as well as the huge volume of unofficial information on the subject is that a lot of myths, hype and inaccuracies have surfaced along the way. There is a real risk of organisations making decisions based on inaccurate or ill-informed information, which not only impact said organisations, but erode the spirit of what the GDPR is about as well.

Uncovering the myths

Over the past year we've heard hundreds of examples of this but, here and now, let's bust the **top 10 GDPR myths** as we've encountered them. As with most things to do with the GDPR, these are generalisations and won't cover every scenario.

1. "What's the point of doing this? One infringement and £17m fine and we're out of business!"

I'm sure we all know by now that yes, a supervisory authority (the ICO in the UK) can issue fines of up to €20m or 4% of group worldwide turnover. There is no doubt that it's a considerable step up from the £500K level that fines maxed out at under the old DPA. But, let's be serious here; the supervisory authority is responsible for "policing" the GDPR. They have a responsibility to ensure that any fine is fair, proportionate and dissuasive. A minor infringement from an organisation that can demonstrate its efforts to comply and co-operate with an investigation are unlikely to be hit with the top-tier fine; just as to-date, to the best of my knowledge, no organisation has been hit with the maximum fine under the DPA.

Furthermore, with the GDPR, another organisation sits above the supervisory authorities. The EU Data Protection Board has the responsibility to ensure equal treatment and application across the member states.
There have been many stories that the supervisory authorities will be keeping the fines, but this is not true. The funds do go to the state, although granted, each member state has to ensure that its supervisory authority(s) are adequately funded to comply with its obligations. It is true that under GDPR the requirement to register with a supervisory authority is relaxed and, in the case of the UK, cuts out the £35 per annum fee to the ICO. It's also true that the ICO are looking at other registration requirements to bridge this gap.

Ultimately the key point is that the supervisory authorities want to try to ensure compliance with the law, not put companies out of business. In my opinion, the reputational damage and potential class action fallout of a breach is likely to be far more damaging and costly than any formal fine, if an organisation has tried to comply and more importantly can demonstrate it.

***Since the time this was drafted, the ICO have issued a statement to equivalent effect.*

2. "These are huge sweeping new changes, how can anyone be expected to comply in time?"

The GDPR does indeed make a number of changes when reviewed alongside the withdrawing DPA, however, the vast majority of it is broadly the same. Unfortunately, the reason it might appear to many that there are major insurmountable changes organisations will have to make to get compliant, is that they were never compliant with the old legislative principles. This is in no way just restricted to the recruitment industry.

At a recent cyber security conference, it was estimated that the majority of organisations would simply not be able to get sufficiently compliant before May 2018. It's the word "sufficiently" that's interesting because aside from the absolutes, the GDPR uses a lot of ambiguous terms such as "state of the art" and "appropriate technical and organisational means." Clearly, what is considered state of the art and appropriate for Microsoft might well not be the same for a small boutique recruitment agency.

Does this mean we can all sit back and say that we won't bother, as a good number of businesses are unlikely to be compliant? No. If you do that you won't have a leg to stand on! If you are progressing with your compliance and can demonstrate this (see a pattern here?) then you may well stand on much better ground.

3. "The legislation only applies to data collected after May 2018."

I'm afraid this is incorrect as the GDPR applies to all of the applicable data your organisation controls or processes, regardless of its age. It has led to wild stories that agencies have to delete all their data and start again, but this too is clearly false. You do need to have a valid legal basis for processing (including storing) any personal data.
It may well be that your interactions with all your contacts and candidates (not forgetting staff) historically meets the requirements of the GDPR. If so, congratulations, although you will be in the minority.

For everyone else, you need to be asking yourself if you really need all that data? If you believe you do, you need to be comfortable and be able to demonstrate that you have sufficient grounds to continue processing. This might be via consent, legitimate interest or contractual for example, although they each have their pros and cons (see later).

Remember, this means that you have to be fully compliant, so you can't just decide to use legitimate interest, for example, and not then ensure that the data subjects have been informed of their rights and that you have complied with transparency rules and so forth.

4. "I can't have my organisation's non-EU team accessing our global database."

This is a little more tricky. If a database is accessed around the globe by members of a specific organisation or group then it could be achieved in a number of ways:- If we had XYZ Recruitment PLC, which owned XYZ UK Ltd, XYZ Inc & XYZ Pty sharing the same database, then you could use the mechanism of "binding corporate rules".

You could also use model contract clauses, although any deviation of these needs to be approved by a supervisory body. Transfers can be used with the data subject's explicit consent, although this is subject to member state derogation under the GDPR, so check that this is allowed in your territory. Ultimately, always remember that the controller has to ensure adequate protection for the data wherever it goes or is used.

5. "I've got to hire a Data Protection Officer now."

This is a common misconception and the confusion around it is understandable. The ICO have released guidance on the topic, but the key factor for recruiters is that there is still no specific definition of "large scale." It relates to the legislation referring to the need for a DPO where (amongst others) "core activities require regular and systematic monitoring of data subjects on a large scale." We've spoken to over half a dozen legal firms and had half a dozen different answers, but the general consensus is that it constitutes between 5,000 and 10,000 records in a database (previous drafts of the GDPR had >250 and >5000, so this feels about right).

The recent guidance from the ICO gives examples such as a single GP doing day to day processing wouldn't qualify, whereas a hospital would. One of the important things if you do appoint a DPO is that it can be done by existing staff (providing they have the right levels of knowledge), but they cannot have any conflicts of interest. For this reason it's advised that certain roles are precluded unless you can demonstrate this.

Also, remember that even if you don't legally need to appoint a DPO you can still do so if you wish, which would certainly help keep your organisation compliant. The function can also be outsourced, which for some reason is proving popular at the moment(!) but there is growing concern that the outsourced DPO functions which serve too many clients, may not be able to respond appropriately when an organisation needs them to.

6. "But that means I can't use my CV parser/database search anymore."

This stems from one of the data subject's rights related to automated decision making and profiling.

Essentially, it means that a data subject should not be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significant effects. Firstly, is any decision impacting someone's chances to be put forward for employment a "similarly significant effect?" There are mixed views from the legal profession, but the good news is that guidance is expected very soon (if not already published by the time you read this) from the ICO.

If this view is held up, then it's conceivable that an agency which automatically parses a CV and inserts it into a database without review, and who then relies on this parsed data, e.g. via CRM searches to produce job shortlists, could fall foul of this.

Before you all groan, it's worth noting that this right does not apply if it's necessary for the performance of a contract between the subject and controller or is based on explicit consent.

7. "I can/can't use consent/legitimate interest/contractual as lawful grounds for processing of data."

First and foremost, if you pick a lawful ground for a specific task in data processing, you can't chop and change.
For example, I ask an existing candidate for consent to continue holding their data. If they fail to give me this consent, I can't then decide to try to process them using legitimate interests. Contractual grounds is the easiest approach, but your rights to process the data are in line with that contract. Once it ends, you need to find another method (or ideally get the candidate on another contract!).

Consent is one of the safest grounds as it removes a lot of ambiguity when done correctly, but the biggest issue is that you have to have "opt-in" consent. Organisations that have built up databases of many thousands of candidates may find that after an opt-in consent exercise their databases are considerably smaller. This has naturally caused a lot of concern, but I would suggest that if a pragmatic view is taken of the data, how many of those candidates are truly active and in regular communication? A database of consented candidates means they *want* you working with them.

Legitimate interest is gaining favour as it's still more in-line with "opt-out" rather than the "opt-in" of consent, but in order to use legitimate interest grounds you have to undertake and document what's known as a balancing test. This can be a challenging test, and is designed to ascertain if your interests in processing the data conflict with any impact to the subjects, and their expectation of what will happen to their data.

One common misconception with legitimate interest is that if you have not collected the data directly from the subject (say via LinkedIn or similar) you might not need to inform them. This is absolutely incorrect. Under the "right to be informed" you must tell the subject that you have their data and provide them with a privacy notice, as well as or including transparency information and their rights to be forgotten or object within a reasonable time. This reasonable time is no later than one month, at the time of first communication or before data is disclosed to another recipient (e.g. your client).

This clause has also led to some interesting interpretations, yet our conversations with the ICO indicate that given the technologies that are available (e.g. email, phone, 1st class post), it is reasonable to inform the data subject you have their data as soon as practically possible. Again, the analogy used is that if you delay and were breached and you hadn't complied with the subject's rights, it's not going to be the smoothest of investigations.

8. "I don't have to worry as one of my supplier's products guarantees my compliance."

This is absolutely not true. Your obligations under the GDPR apply to your entire organisation and cover both physical and electronic data as well as its security. Only you are responsible for this, as only you determine the purpose and means of processing the data you hold. Many suppliers will be adapting products and services to *help* you with elements of ensuring the way your organisation is run falls in line with your obligations, but no-one can guarantee it.

For example, your CRM supplier might add features to support your processing of candidates, but it's unlikely to handle the physical security of your office or handle the retention policy of your share certificates. In certain circumstances, suppliers can jointly be responsible for very select elements of shared liability. An example might be a CRM supplier storing your CRM data on a SaaS solution, but this is limited.

9. "My sales prospects are/aren't personal data and aren't covered by the GDPR."

There are no two ways about it that this is one of the most confusing aspects at the moment. The reason is that there are a multitude of potentially conflicting directives and regulations around marketing. Coupled with the ability for member states to put their own interpretation forward in certain cases, the result is that you're none the wiser.

You have the GDPR vs PECR (Privacy and Electronic Communications Regulations) combined with the current B2B member state exemption (e.g. UK and Ireland). There is no doubt that GDPR catches the data typically held when used in direct marketing and so it must be protected appropriately. The B2B exemption only applies with the need to obtain consent before emailing businesses with direct marketing. At the time of writing it is believed, but not confirmed, that this exemption will persist beyond May 2018. Formal guidance from the ICO is due on this.

10. "Why are we going through this now, yet more red tape and confusion, this is highly detrimental to my business."

This isn't strictly a myth, since if you are taking it seriously it is likely to be impactful, but what about the mid to long term view? There are many examples out there where breaches have devastated businesses (TalkTalk, Ashley Maddison, Target…), and proportionate to staff number and turnover of an organisation vs amount of PII information held, the recruitment industry is one of the largest.

Recruitment is also one of the most competitive and legislation-bound sectors to try and do business in. It is also one that, unfortunately, seems to pick up more than its fair share of bad press. There's an apparent increase of complaints against agencies of spamming, and data subjects (remember that's candidates, contacts and staff) will only get more aware of their rights, which also remember, includes compensation.

It is a fact that the threat to your business from cybercrime or data subject based claims will increase. Data protection legislation is designed to try and protect both sides of the equation, the controllers and processors as well as the data subjects. Embracing this in what for many of you will be a cultural shift now and possibly painful in the short term, could well make you more competitive, more resilient and give you a far better platform to grow securely from in the future. One of the key challenges for any business will be the requirement to demonstrate their compliance from every angle.

This means a lot of tracking and auditing will be required; the GDPR gives several examples where it suggests providing data subjects the ability to interact with your business through, for example, a portal or website to manage their data interactions and receipts with you to make this process less labour intensive.

Conclusion

To summarise there's a lot of hype and sensationalism about GDPR and some of it is even accurate(!). There's no doubt there is a lot for most boards of directors to come to terms with, and a lot of effort and resource could well end up being spent over the coming months. The key thing is not to panic (yet), but if you haven't started looking at what impact the GDPR and other current and forthcoming data protection and privacy legislation will have, then I urge you to start now.

OTHER RESOURCES

Webinars

In addition to this whitepaper, Paul Mather has written and hosted a series of webinars on the GDPR.
You can view/download a copy of each webinar by clicking on the relevant titles below:

- **GDPR PART 1 - OVERVIEW AND KEY POINTS**
- **GDPR PART 2 - RIGHTS AND CONSENT**
- **GDPR PART 3 - LEGALITIES, POLICIES AND PROCESS**

Articles

For articles written by Paul Mather go to - http://insights.voyagersoftware.com/u/102e6gm/paul-mather

LinkedIn

We've created a specialist GDPR Information and Discussion Forum on LinkedIn for you to join. Therefore, should you have any questions on the whitepaper or would like to connect with fellow professionals to discuss the elements of GDPR and how it could impact your business, then please go to - https://www.linkedin.com/groups/8599770

You can also connect with Paul Mather directly through his LinkedIn profile - https://www.linkedin.com/in/paulmather1/

This whitepaper is provided for information purposes only and is NOT intended to be legal advice pertaining to the subject matter.
If you have specific questions on how this may affect your organisation you should consult a legal professional.