Finding the Right GDPR 'Expert' to Help Your Business

October 2018

CONTENTS

EXECUTIVE SUMMARY 2
ADDRESSING THE CHALLENGE / BRIEF HISTORY OF PRIVACY 3
WHAT DOES A GDPR PROJECT LOOK LIKE? 5
Step 1: Prerequisites 5
Step 2: Data Discovery 5
Step 3: Process Mapping 6
Step 4: Lawful Basis for Processing 6
Step 5: Documentation 6
Step 6: Operationalise 7
THE THINGS YOU NEED TO KNOW 8
SUMMARY 13
ABOUT FROUD 14
ABOUT CORE CONCEPT SECURITY 14

EXECUTIVE SUMMARY

The introduction of any new law/legislation is going to elicit a response from individuals and organisations trying to make money from the ensuing confusion and possibly panic. Filling the voids is the very nature of our economic system and I have absolutely no concerns when this is done *well*.

When the individuals or organisations have the necessary skills and education, a proven track record, and an honest desire to help, the services and guidance they provide are as necessary as they are critical. It's when they do only the bare minimum to *appear* qualified that the problems start.

From aggressive marketing and PR campaigns selling fear uncertainly and doubt, to meaningless qualifications, to get-compliant-quick schemes, countless millions have already been thrown away on wasted effort. Or worse, the *wrong* effort!

Integrity, it seems, rarely takes precedence over profit.

However, like every other service, the hiring of the *right* GDPR expertise for your business is about *your* ability to ask the right questions. While no one can just give you all those questions up front - you must do some homework for yourself based on your unique scenario - this white paper should provide enough to at least get you started.

I've said a thousand times; if you have never even *read* the GDPR you will never be able to obtain the right help at the right time.

These links are a good place to start if this is all relatively new to you:

ICO - "Guide to the General Data Protection Regulation (GDPR)"

Bird & Bird - "Guide to the General Data Protection Regulation"

Froud on Fraud – "Free Resource: The GDPR in Plain English"

Good luck!

ADDRESSING THE CHALLENGE / BRIEF HISTORY OF PRIVACY

Everyone has heard of privacy, but I think it's fair to say that far fewer people can *define* what it means in the terms used in the creation of new laws and regulations. The description is quite important, and has its foundation in Article 12 of the Universal Declaration of Human Rights (UDHR);

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

Everything in the GDPR stems from this basic premise and is the distillation of a significant amount of work over the last 70 years since the UDHR's proclamation in December 10th, 1948.

For example, here in the EU:

The intent of the above human right was, in turn, ratified as Article 8 in the European Convention on Human Rights (ECHR) on the 3rd of September 1953;

…which was expanded into the 8 Principles put forward by the Organisation for Economic Co-operation and Development (OECD) in "The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" on September 23rd, 1980 (and should be very familiar to anyone who has read the GDPR):

Part Two. Basic Principles of National Application

- *Collection Limitation Principle*
- *Data Quality Principle*
- *Purpose Specification Principle*
- *Use Limitation Principle*
- *Security Safeguards Principle*
- *Openness Principle*
- *Individual Participation Principle*
- *Accountability Principle*

…and ratified in the Charter of Fundamental Rights of the European Union (CFREU), or 'The Charter' eventually entered into force on December 1st, 2009:

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority*

…and all are now distilled into the GDPR, which is to be adopted by *every* organisation within the scope of Union law.

However, even familiarity with all the above does not actually *help* organisations now legally obligated to comply to achieve compliance. Privacy / data protection expertise is a speciality, like anything else. You either have it or you don't.

If you have it, great, carry on, if you don't you need to find people who do. Not a single person, PEOPLE! There is no-one I have ever met who has the skill-set to do everything, which includes;

- Project definition in-line with line of business, industry sector, and region;
- Project Management;
- Policy Creation and Implementation;
- Contract Creation and Negotiation;
- Information Security;
- Data Protection Impact and/or Legitimate Interest Assessments (where/if applicable);
- Definition and documentation of justification for lawful basis for processing;
- Creation and submission of Record of Processing Activities (if applicable)
- …and so on

On the other hand, you will only want to commit to an expense and level of effort that is *appropriate* to your unique organisation. There is no one-size-fits-all, and very few vendors will stop you from spending more money.

But that's exactly what you need, and you will only get it by asking the right people the right questions.

This white paper is a start, but it is entirely up to you to make the questions bespoke to *your* organisation. Some questions will be more important than others, just as some answers will take on a whole different meaning between disparate organisations / industry sectors / regions.

And given that the whole concept of compliance within the realms of privacy is still relatively new, few organisations can answer all the questions to a degree you may wish. If they can, it's unlikely you'll be able to afford their services. However, you will certainly be able to determine those who are talking utter nonsense.

In the end, there is no better way forward than doing some homework.

WHAT DOES A GDPR PROJECT LOOK LIKE?

Before you even begin questioning the prospective GDPR consulting companies, we must first put the *project* to achieve GDPR 'compliance' into a little perspective. And you as the reader will need to accept – perhaps with a few organisation specific differences - my description of a GDPR project done well.

At a very high level, a project *should* contain all the following.

Step 1: Prerequisites[1]

1. READ IT! - There is not one person who does business with organisations 'established in the Union' to whom the GDPR does not apply. You are responsible in some way of ensuring other people's personal data is protected, and you should be aware of *your* rights when it comes to your *own* data;
2. Senior Leadership Buy-In - Like everything else, if the top people in an organisation are ignorant and/or ambivalent on a subject, nothing will happen. Your Board of Directors don't have to be GDPR experts themselves, but they had better take it seriously as they will ALWAYS be held liable if things go wrong. You can outsource a large part of the of GDPR *function* (even the DPO), but never the *accountability*;
3. Stakeholder Training - This can be as simple as a one-day engagement where an appropriate representative of each departmental vertical (HR, Sales, Operations etc.) undergo GDPR training bespoke to *their* business needs;
4. Designation of Project Ownership - If you already have a Governance function, this is easy, just give it to them. If you don't, you will have to assign the initial project to someone with enough knowledge AND influence to be effective;
5. Wider Business Context - You must first decide on your objective: Regulatory compliance? Best in class? Best in the world? e.g. if you are functioning as a 'Processor', then your prospective client's policies and SLAs may go well beyond minimum legal requirements.

Step 2: Data Discovery[2]

Even if it's too late to perform the above step, and especially before you begin questioning the prospective *legal* experts, you must know what personal data you've got, and what you're doing with it.

Under GDPR you are responsible for (amongst other things):

1. Determining your lawful basis for processing for each of your separate business processes (both internal and client facing);
2. Implementation of data subject rights in-line with 1. (erasure, portability etc.);
3. Data minimisation (during collection and data retention);
4. Data confidentiality, integrity, and availability (all to defensible levels);
5. 'Legitimising' all transfers of, and responsibilities for, data to third parties / third countries

You must therefore run some form of data discovery exercise, which generally consists of one or both of:

1. Running a series of interviews and questionnaires with all unique departmental stakeholders to

[1] See *GDPR Compliance Step-by-Step: Part 1 – The Prerequisites*
[2] See *GDPR Compliance Step-by-Step: Part 2 – Data Discovery*

manually track and map the data; and/or

2. Running some form of data discovery technology to find the data on end systems / databases / other file stores etc.

Step 3: Process Mapping[3]

If you have performed the data discovery exercise laid out in the previous section, you will now have a bunch of data with only limited context. For data to become *information*, you need to provide the appropriate context, which in GDPR terms, is in the form of a 'business process'.

Every one of these individual business processes requires its own determination of lawful basis for processing.

e.g. HR will have processes for Recruiting, On-Boarding, and Benefits; Sales will have Current Client Management, New Client Prospecting, and Telesales; Marketing will run campaigns based on data from past/present/future clients, and so on.

Step 4: Lawful Basis for Processing[4] [5]

While some scenarios would seem to be obvious; like doctors requiring personal data for vital interest, lawyers requiring personal data for legal reasons, or service providers requiring personal data to fulfil a contract, the devil is in the detail. Getting this wrong not only has a direct impact on your ability to demonstrate 'compliance', but you may also be implementing all the wrong controls.

However, the lawful basis can have a significant impact on the technical and organisation measures you must put in place, so consideration must be given to things like:

- *Determine if it's the RIGHT decision* - Lawyers are only going to make decisions based on the facts / evidence provided in the Process Mapping step, they will likely have little insight into [or care about] the criticality of the business process in question. Or of the impact changes will have on the business;
- *'Minimise' what's left (Data Categories)* - Data Minimisation is, by itself, one of the 7 Principles of GDPR, and the less data you have, the fewer things you have to do with it;
- *Consolidate what's left (Data Sources)* - Just because you need something, does not [necessarily] mean that you need several copies. You only need ONE production copy of something (along with all requisite access and resilience obviously);
- *Shut down / amend the legacy data acceptance channels ("stop the bleeding")* - Now that you've worked out what you need to keep, stop the bad stuff coming in.

Getting to the lawful basis for processing is often confusing and difficult and involves the entire organisation in some way. Don't try to run a GDPR project in a silo.

Step 5: Documentation[6]

Documentation is your evidence of compliance. It's as simple as that. Even if you're lucky enough not to have to maintain 'records of processing activities' (see Article 30(5)), you still must document everything else, including WHY you don't think you have to maintain records!

---

[3] See *GDPR Compliance Step-by-Step: Part 3 - Process Mapping*
[4] See *GDPR Compliance Step-by-Step: Part 4 - Lawful Basis For Processing*
[5] See *GDPR: Getting to the Lawful Basis for Processing* for instruction and samples
[6] See *GDPR Compliance Step-by-Step: Part 5 - Documentation*

The word "appropriate" appears 115 times in the GDPR final text, and "reasonable" a further 23 times. It is therefore very clear that the determination of whether what you're doing meets the *intent* of the law is just as important as meeting the *letter* of it.

At a minimum you will require:

- *Policies* - Including those covering Data Protection / Privacy, Employee Privacy, Third Party / Third Country Transfers, Data Subject Rights, Information Security, Vendor Due Diligence and so on;
- *Personal Data Assets* - Steps 3 and 4 above should be documented in detail and all data stores recorded in an appropriate asset register;
- *Lawful basis for processing and corresponding data subject rights* - These must be clearly articulated and match the information contained within the Personal Data Assets;
- *Technical & Operational Security Measures* - If you haven't already documented your *entire* security program against a standard *like* ISO 27001, you will need to;
- *Records of Processing Activities* - With a couple of caveats, if your organisation has fewer than 250 employees you do not need to record this, otherwise you will need to record everything your local supervisory authority requires of you[7]

Step 6: Operationalise[8]

If you don't build the necessary knowledge / processes into everyone's day jobs, your GDPR compliance program will falter. While data protection and privacy are everyone's responsibility, they cannot, and will not be at the forefront of everyone's mind as they work through an ordinary day.

You will also have pretty much thrown away everything you did on the first 5 steps.

These are the things that will need to be operationalised:

1. *Governance*
2. *Policies, Standards & Procedures*
3. *Employee On-Boarding / Awareness & Training*
4. *Risk Management*
5. *Asset Management*
6. *Vendor Due Diligence*
7. *Incident Response / Breach Management*

Where possible the above should be filled with existing personnel, it's only the gaps were trying to fill here. But until the entire project is mapped out to the above steps, or at least something like it, the below questions will have no context.

Finding the right questions to ask your prospective consultants means already knowing what the answers should be.

[7] The UK's ICO provides samples and guidance *here*
[8] See *GDPR Compliance Step-by-Step: Part 6 - Operationalise*

THE THINGS YOU NEED TO KNOW

The questions below are designed to be generic enough to suit almost any business, as well as potentially form the core questions of your Request for Proposal (RFP);

1. How long have you / has your company been in business?

   A company that has been in business for only a few months is generally a higher risk than one that's been in business for a decade, especially for a long-term project such as achieving GDPR compliance for the first time. That's not to say you should *automatically* exclude new businesses (they have to start somewhere), but do they at least have a verifiable history of providing these services? If no, and they cannot provide CV/resumes of consultants who *have* provided these services, there's a good chance they jumped on the GDPR bandwagon.

2. How long has your company been performing data protection/privacy consulting, including GDPR?

   Notice I say "including" GDPR, as this is not the only service they should be providing, or at least have access to (through partners and/or subcontractors). The Recitals and Articles of the GDPR represent only a single aspect of an effective and overarching corporate governance function. A very important part yes, but before spending significant time and money implementing GDPR, the program must be put into an appropriate business perspective and context.

   Also, unless consulting companies are formed of experienced multi-disciplined practitioners, they may not have what it takes to perform the entire assessment effectively, or efficiently.

3. What is / are the education / experience / qualifications of your consultants?

   The GDPR is bringing more charlatans out of the woodwork than any regulation before it. Privacy / data protection is a career in and of itself, not a bullet point on a CV/resume! It's also an entire facet of the law, as are all other human rights and cannot be learned in a matter of weeks. Yet millions are being spent on consultants with no more experience than that provided by a few hours reading and a meaningless certification.

   I am of course talking about the GDPR Certified Practitioner and equivalent, and data *security* consultants suddenly adding privacy to their list of proficiencies / expertise. It simply does not work that way. Yes, they may have a critical role to play, but they cannot play *every* role and should not even try. You must separate the wheat from the chaff.

   In other words, GDPR/privacy *lawyers* will help you to determine what you need to do, and, the GDPR/privacy *consultant* will help you figure out how to do it in practice.

   The right help depends on what stage of the project you are in, and the right questions must relate to specific deliverables within that project.

4. Have any of your consultants completed an Article 30 Record of Processing Activity (RoPA)?

   Not every organisation has to maintain Records of Processing Activities per GDPR Article 30, let alone submit them to a supervisory authority (e.g. the Information Commissioner's Office (ICO) in the UK). However, every organisation is still held accountable for being able to demonstrate appropriate compliance with the regulation if required. The RoPA represents the high-level snapshot of all the effort you have expended and should be part of the final report due at the end of a GDPR engagement. The RoPA is the GDPR 'holy grail' in the continuing absence of a

certification mechanism.

You need to be able to go from project inception all the way to a RoPA (or equivalent), so you are probably best served by consultants who have already made the journey. They've been there and done that, so there's a far better chance that they can eventually do so on your behalf.

5. How many assessments has your company performed in my business type / industry sector?

Performing an assessment on a relatively small e-commerce merchant is very different than one performed on a large multi-national. Unless the consultant has performed assessments on your type of business, the service could be less than optimal, potentially causing issues down the road.

The reason I ask how many assessments the *company* has performed, and not the individual consultant is because an assessment should not be performed by a single 'expert' alone. No one can do everything. Yes, you may have a single focal point / point of contact, but no single consultant has the necessary skills to assess your entire business adequately against all GDPR requirements. Every consultant has a unique skill-set, so your consulting company of choice should have a sufficient *mix* of skill-sets to cover your entire organisational needs or have partnerships with those that fill those gaps.

6. Describe your methodology for gathering the information necessary to make determinations of the legal basis for processing?

This is really where the rubber meets the road in any GDPR project. The whole point of the exercise is to make each of your individual business processes that involve personal data 'legal'. No privacy expert can do this without receiving a list of very specific, and well-defined fundamentals (e.g. purpose of processing, categories of individual, category of personal data, controller/processor etc.).

Every project is just a series of action items that are defined, assigned, and tracked to completion. A GDPR project is no different, so unless the organisation you hire has a *plan*, compliance will end up becoming an ever moving goal, defined by frustration and scope creep.

It may well be that you end up hiring a number of consultants based on their individual skill-sets, but you *still* need an overarching plan in order to put their work into the appropriate context.

7. How do you maintain the continuity of an engagement?

Given 4. above, it is very likely that different consultants will take the lead at the different phases of a GDPR project. How do you maintain the continuity of the assessment process when there is so much information in the previous consultant's head? Does all that knowledge go with them, or is the assessment process itself so well organised that the information is ready to hand?

Unless you are satisfied that the assessment process is backed by a tried and tested methodology, this unfortunate (but frequent) issue may raise its ugly head. At the very least ensure that any time spent bringing the new consultant up to speed is at the other company's expense, not yours, as the ensuing delays can be extensive.

8. How do you deal with the differing opinions of your consultants?

This question speaks to consistency, the experience of the individual consultants, and the maturity of the consulting company as a whole. Bottom line; any opinion from any consultant should have the backing of their organisation, especially where significant capital or resource costs expenditure is required. The GDPR itself is actually open to a great deal of interpretation

(define 'appropriate' for example?), so any decisions made by one consultant must be agreed by them all.

Unless the consulting company has a formal process for accepting their consultant's decisions, in writing, and backed by contract language, you'll want to keep looking.

This does not help you maintain consistency from one consulting *company* to the next, so your previously supported opinions should be documented and agreed beforehand.

9. Do you have communication SLAs?

The is nothing more frustrating than having your point of contact resemble a black hole to your communication attempts. Have reasonable expectations but insist that an SLA be built into your contract.

Something as simple as agreeing that receipt of all emails will be confirmed within 24 hours is a start. However, if you have outsourced you DPO function, this is no longer a nice to have, but mandatory.

10. Do you provide any other compliance or security related consulting services?

The GDPR is very specific to personal data. Too specific in fact to cover the compliance or security needs of all the sensitive data types you have in your systems. Do you have corporate financial data? Intellectual property? Spending money on GDPR and not including ALL your businesses sensitive data is probably not the best use of your budget.

If required, in choosing a consultant make sure that they have the necessary experience in dealing with other forms of data which may be covered by non-GDPR regulatory or compliance standards (the PCI DSS, or HIPAA in the US for example).

11. Can you recommend products or services to help us achieve compliance?

Be very careful here. For a lot of companies, the consulting aspect of a project is just a means to an end, and that end generally involves selling you a bunch of their OTHER products or services to 'help' you achieve compliance. Especially technologies or managed services.

Review their website carefully, what are your first impressions? Are they a service company designed to provide impartial and expert guidance or are they a product company disguising themselves as 'privacy experts'?

There is absolutely nothing in the GDPR that states that a single organisation can't do everything for you, especially in terms of your technical and operational security measures, but common sense suggests this is very likely a conflict of interest. Your vendor program may be easier to maintain, but does this complete absence of checks and balances fit with your policies or operational practices?

The answer to this comes back to your view on privacy itself; are you doing this just for compliance, or because it's the right thing to do?

Last warning about these additional services; they must support *your* GDPR compliance, so any organisation providing them will need to be compliant themselves, and back it up in appropriate contract language and SLAs.

12. How do we *maintain* GDPR compliance?

So, you've achieved compliance, now what? All compliance means at the end of your initial project is that at a SINGLE point in time all the required controls were in place. It does not necessarily mean that these controls are in place on all the systems, all the time. They need to be.

GDPR compliance without *some* form of management systems in place as a wrapper around them is almost pointless. You are no better off than you were before, and you will probably have to expend the exact same effort to 're-certify' your compliance as you did achieving it in the first place.

As part of a good consulting service, your consultant should at least have a plan to help you take your GDPR compliance project and develop it into an enterprise-wide data protection framework. Whether you choose this route or not, you should at least have the option to do it later.

13. If we cannot meet every regulatory requirement, then what?

There is no pass/fail in GDPR, your compliance is tied to your ability to justify that what you are doing meets the *intent* of the regulation. (i.e. is it 'appropriate'?) Therefore, it is important to get qualified help as the intent of GDPR will be all but lost on those without the appropriate background.

That said, having *any* plan - even a multi-*year* plan - is better than having no plan at all, so don't get caught in the loop of 'analysis paralysis'. You must be seen doing *something*!

14. Can I interview your consultants first?

Insist on interviewing a couple of the potential consultants per company and have a list of questions most important to YOUR business already prepared. If you don't like the answers, or if the candidates do not give you the warm and fuzzies, move on.

They do not have to know the answer to all your questions, but they do have to be completely up front with you. It's OK not to know something if you know someone who does. That's what consultancy is; knowing where to get the answers.

For example; If you were to ask, "To whom does the GDPR apply?" and the answer was "To all EU citizens.", you will know to move on.

15. How does your organisation stay up to speed with developments in the field?

Even though the GDPR's predecessor; the Data Protection Directive (Directive 95/46/EC) had much the same content, it was minimally enforced. It was also enacted differently in all 28 EU countries. Hence the necessity for 'harmonisation'.

What this means in reality is that there is limited precedent on HOW to enforce the GDPR, or to develop the additional requirements. Certification for example. It is therefore critical that an organisation charged with helping you achieve compliance, knows what compliance *looks* like at the time. In *your* industry sector, and *your* region, and so on.

Privacy is also rapidly expanding outside of GDPR and if you are operating in any other territories then knowing how to avoid parallel efforts and be compliant in multiple jurisdictions requires constant monitoring of the regulatory environment.

16. How long does it take to get compliant?

    Impossible to answer without a LOT more information. Immediately dismiss any consulting company that gives you an up-front timeframe.

    Besides, this is not a ‘one-shot’ effort, GDPR requires *continuous* compliance and the end of project is should really be marked by self-sufficiency, not a piece of paper.

    This a 'trick' question designed to weed out the worst offenders.

SUMMARY

Choosing the right GDPR expertise for your unique needs can seem daunting, especially if you do not have a data protection specialist on staff. However, if you keep the following points in mind, and ask all the questions above, you should be able to choose the best help for your business goals;

1. GDPR is about the implementation of human right, not just lip-service or summary nod to corporate responsibility. The penalties indicate just how seriously this law is taken;
2. GDPR is not about 'compliance', it's about legally processing personal data and securing it to a degree appropriate to the risks involved;
3. A GDPR 'project' conducted outside of existing business process / risk management program could be a waste of time and money;
4. GDPR controls without the management systems to maintain them, will not keep your data processing 'legal' or your data secure, let alone keep you fully compliant;
5. Don't start a GDPR project until you have done a Risk Assessment, a Business Impact Analysis, AND a scoping exercise;
6. **GDPR must fit into your business, not the other way around!**

ABOUT FROUD

David has almost 20 years of experience in areas of Information / Cybersecurity, including Regulatory Compliance, Secure Architecture Design, Governance Framework Design, Data Privacy & Protection, FinTech and Sustainable Innovation.

As Project Lead for several Fortune / FTSE 'Enterprise Class' clients, David has performed hundreds of on-site security and compliance assessments for organisations globally.

Blog: http://www.davidfroud.com

Linkedin: http://www.linkedin.com/in/davidfroud

ABOUT CORE CONCEPT SECURITY

Core Concept Security (CCS) is an independent cybersecurity and data protection consulting practice based in the UK, but available globally.

The guiding principle behind all CCS's services is that security, while difficult to achieve, has always been and will always be, simple. There are no shortcuts to security, and there is nothing to be gained by just throwing money at it hoping the problems will go away. Technology will never fix what's broken, only people and process can.

The CCS approach is also simple; It's our job to help you ask the right questions, even if we aren't the ones who can actually answer them. We are just as happy to point you to someone who can.

In the end, if your security program is not appropriate to your business needs it is a waste of your time and effort. Our commitment to our customers is to never settle for less than, or try to sell you anything *more* than, what you need.