THE GDPR MATURITY FRAMEWORK

A proven methodology for unlocking the power of personal data in order to build deeper digital trust in accordance with the GDPR
The major challenge with designing, implementing and complying with GDPR legislation is knowing what good looks like; how do you know when you’ve got there? What is best practice? And how do you know when you have reached the point of appropriate and proportionate risk-based controls, especially given competing business demands and ever-increasing privacy-expectant customers and clients.

Each organisation needs to know when good-enough or best practice is achieved and, crucially, where to draw the line and where to continue focusing effort or how to maintain compliance once they have implemented GDPR requirements.

This GDPR Maturity Framework is a result of a collaboration between a team of highly experienced privacy and security professionals, lawyers and regulators. Directly stemming from this work comes a level of functionality that means any organisation—regardless of shape or size—can calculate what ‘good’ actually looks like.

You can now judge if you have arrived at that point, make meaningful comparisons against similarly sized companies, how you rank against your peers, and, critically, you can work out how to achieve and maintain a strong defensible position following the five easy steps contained within the following GDPR Maturity Framework.

In May 2018 we saw the go-live of the most significant change to data protection laws in twenty years. Nearly every business and organisation that has personal data relating to living individuals within the European Union (that’s 32 countries or 0.5 billion people), has had to ensure compliance with this new General Data Protection Regulation, or ‘GDPR’.

This new law has also ramped up the power of the individual and in doing, has placed a significant data administration burden on every business and organisation that processes personal data.

These developments have seen the role of the Data Protection Officer (DPO) suddenly thrust into the lime light and having to answer tricky questions like “how and when will we be compliant with GDPR?”

This white paper provides an overview of the GDPR Maturity Framework that helps a DPO, as well as the organisation, navigate through the complexities of data protection, privacy and security on a global basis.

Steve Wright
Privacy Culture
There are broadly three risks that we now recognise as the driving force for GDPR compliance... 

01 Risk of Reputational Damage

The Talk-Talk mobile phone operator breach in 2015 is reported to have cost £60m to fix and the share price dropped 20% at the time of the announcement. Conservative estimates put the cost of the personal data breach in excess of £120m in lost revenue and the amount of money it cost to re-acquire lost customers who needed significant discounts in order to be enticed back.

Reputational damage can sometimes be so severe that it can kill a business. Not only that, businesses now face the wrath of the Regulators, who can make their data mishandling and data loss mistakes very costly.

02 Risk of Prosecution, Fines, Litigation and Class Action

Fines of between 2 and 4 percent of global turnover or €20m–whichever is the greater–can now be applied by any of the EU Regulators on the basis of being found non-compliant with GDPR or following a significant data breach / loss.

Every organisation that processes personal data must demonstrate and verify that it has complied with these higher standards. This can’t be left to luck or chance, so implementing a maturity framework will remove the guesswork from the equation.

To date, there have been a dozen such cases, with fines totalling £55m; albeit £50m was CNIL fining Google.

03 Risk of Damage to Businesses & Individuals

Under the GDPR, every EU citizen now has a deeper degree of control over their personal data, with a plethora of beefed-up personal data rights. Should an organisation fail to uphold these rights, or should it fail in its responsibility to safeguard the personal data, then the individual can now take legal action.

The Morrisons Supermarket data loss was the first such case, where 5,500 staff brought a claim for compensation. Morrisons were found to be ‘vicariously responsible’ by the High Court and Court of Appeal; although the UK’s fourth largest grocery chain was given leave to appeal to the Supreme Court.

General Data Protection Regulation (GDPR)

This Regulation was adopted in April 2016 and the two year transition period ended on 25 May 2018. It regulates the way in which all organisations can process personal data, how this can be used, the rights that customers, clients, supporters and employees now have in this new data protection landscape as well as how such personal data must be protected and secured. Underpinning the Regulation are three important principles - transparency, accountability and control.
THE 5 STEPS TO CREATING YOUR MATURITY FRAMEWORK

AS SIMPLE AS 1-2-3?

To answer this question, I have been working with a small team of privacy and legal experts to deliver the GDPR Maturity Framework you see before you.

Such a framework should be used to ensure you know when you’ve done enough; when you have achieved ‘good-enough’. It can also be used to measure your organisation against other similar-sized organisations or similar industries.

This whitepaper will walk you through the five easy steps that make up the GDPR Maturity Framework. It’s based on 25 years of pragmatic and practical experience in designing and implementing cyber security and privacy control frameworks. It takes inputs from fellow in-house privacy professionals, DPOs, lawyers & CISOs and it gives what I think is a realistic approach on how to ensure you have done enough to remain compliant with GDPR.

Moving from a Defensible Position to a Satisfactory Position

(Or a Good Enough Position)

I first heard the term ‘Defensible Position’ from a well-known barrister a couple of years ago. He was explaining to me that in order to prepare for GDPR compliance, you have to think like the prosecution or a judge. They look for gaps in your story and try to expose any weaknesses—rather like a hacker would seek to break through your defences.

Over the last two years we have been busy documenting and testing the 12 domains that make up a defensible position, and, in doing so, have created best practice, also known as a ‘satisfactory position’. The GDPR Maturity Framework encapsulates both the ‘defensible’ and ‘satisfactory positions’, it’s been tested across more than 30 complex environments, and more are being added all the time. It has proven to be broad enough for your Board to understand, yet comprehensive enough to test the very best auditors, professional service firms, law firms and, of course, the Regulator, although this is still yet to be fully tested.

The guiding principle, and the first place we start on the road towards being in a ‘defensible position’, is of course Accountability. What does it mean, how can you ensure that your staff feel accountable and know how to be responsible? What instructions should we provide, or should we simply tell people to follow orders? Also, how can governance be effective without overloading an already busy agenda?

If Accountability is our collective responsibility, then how can we ensure that the Rights of individuals are upheld, especially when we have complex legacy data-holding systems that are old and unsupported?

Cyber Security is, and will continue to be, hard-work and a constant battle. So how do we ensure that the most important red-line items are addressed in priority order, at the same time as keeping the good guys safe and the bad guys out?

Above all, if we are going to move towards a ‘satisfactory position’ or be able to Demonstrate Compliance with all these new procedures and new GDPR requirements, then it’s got to start with Training, Awareness and Cultural Change applied across your organisation. In other words, GDPR is only truly effective when you’ve changed the mindset and behaviour of your organisation. Your people need to think about personal data differently, act differently and, of course, continue to be your first line of defence.

Being ‘good enough’ is about adhering to best practices and our GDPR Maturity Framework is a practical tool that allows you to be measured against these these five guiding principles; read more about them in the following chapters.

The House that GDPR Built: It is possible to think of the Maturity Framework as a house built on foundations of Culture, Training and Awareness, and supported by the pillars of Rights, Security and Compliance, all under the protective roof of Accountability.
ACCOUNTABILITY ISN’T ALWAYS the first word we think of when it comes to data privacy or data protection. We tend to think about accountability as being or feeling responsible for something or someone, say a process, people or even a system.

In relation to GDPR, specifically, we tend to frame ‘accountability’ in terms of protecting our data—e.g. cloud or data centres—and ensuring it remains confidential. This is not wrong, but accountability is broader than that; it’s about having a good understanding and knowledge of who is responsible for data, irrespective of whether it sits on systems, data storage or in the cloud. Accountability is all about ownership, responsibility and having strong governance in place.

For sure, we feel very strongly about certain things remaining private and we will defend the privacy of our home against invasion and yet accountability GDPR came into being for exactly these reasons. It wasn’t a dark cabal of Brussels bureaucrats who decided to wrap Europe in red tape. It was created to promote and provide protection for the fundamental human rights and is enshrined in the 1948 Human Rights Act.

Being accountable means that named individuals need to either assign responsibility to someone else and at the very least, be able to justify why they have the data (Purpose), on what legal basis (e.g. Public Task, Legitimate Interest, Consent) they process the data, where and how the data is stored (end-to-end lifecycle), and how long the data will be retained for (Retention & Deletion).

Accountability should be very clearly laid out: not just to the individuals whose data is held, but also the public and members of staff should be able to access information about who is responsible for the data, how to make changes or exercise their rights to it and understand if they themselves are in some way accountable. This is often captured in privacy notices under the heading ‘Transparency’, but it does not end there. Instead, every organisation—be they two men and a dog, or a multi-international firm—should know who the data owners are, where and how the data traverses their network, who has access to it and why, what controls are in place that are appropriate and proportionate to the risks, how long they intend to use the data, and of course, what they do with the data when it becomes redundant.

Accountability can be straightforward, however, in large complex organisations this takes significant work and commitment, as each department or business will have different data needs, they will also have differing ideas about what is ‘good enough’. This is where you need to work hard to demonstrate why having better, more informed metadata, and the legal basis for processing, enables you to deliver greater returns on the data collected in the first place.

Being able to understand this argument is one of the keys to unlocking difficult conversations with reluctant data owners who don’t like being held accountable. In these cases, an RACI matrix can help to ensure people understand who and what they are responsible for and why.

The RACI can also help focus thinking about operationalising the tasks of privacy—which, again, is misunderstood or ill-defined—and tends to cause problems for organisations that are solely focused on the implementation of GDPR and not necessarily how to manage data privacy and data protection.

ACCOUNTABILITY CHECKLIST

Desired State
- A documented governance structure with clear data ownership, and business owners named against every business process and data set in the organisation
- Detailed accountability, ownership, with roles and responsibilities for the different data owners, including data management and which processes utilise the data
- Formal evidence of where key decisions are made, especially where harm to an individual may be applicable or change to the level of privacy risk is unacceptable
- Ability to track actions and changes to the data landscape via the DPA process and updated ROPA
- Data Privacy included on the organisation’s risk register
- GDPR compliance (control) framework, including how each control is being monitored and adhered to
- Data Protection Officer is in place, with appropriate support

Documents
- Data Protection Officer job description and contract
- Operational Procedures including ‘Nominated Data Owners’ and ‘Allocated Business Owners’
- RACI Matrix
- Transparency & Privacy Notice(s)
- Privacy Network—day to day responsibility for data within their Business Area
AS ‘DATA SUBJECTS’ within the EU, we are all entitled to eight fundamental GDPR Rights. However, only some of these rights are new. The new rules include the right to be informed, rights to access and rectification, rights regarding data portability, the right to object and – the really tricky one– rights in relation to automated decision making and profiling, where the potential for misuse or error is formidable.

Interestingly, many of the rights that appear new, were already enshrined in our local data protection laws, but it took GDPR to realise and bolster them. In other words, the risk of flaunting older laws was potentially worth it to some organisations, as the Regulator was pre-occupied with larger cases and any transgressions would have been punished with relatively minor fines.

Thankfully, it was only a small percentage of organisations that blatantly ignored the rules–most small businesses were simply unaware that they had such obligations. To be fair to them, all they knew was that when it came to the collection, storage and access to personal data, the main problems they faced were losing the data to the competition when their sales managers moved on, or if someone accidentally attached the wrong Excel file to an email. But, as we all wait, with bated breath for the first organisation to be dragged over the coals, we’re all now aware that the real law is potentially worth it to some organisations, as the Regulator was pre-occupied with larger cases and any transgressions would have been punished with relatively minor fines.

What does this mean for our organisations? Why should we care? I support several schools on GDPR matters, and as a parent governor, I can tell you these rights are very useful to parents or carers that need access to previously unseen data about their little ones. Unfortunately, this level of access can have the negative side effect of teachers and carers not writing down crucial information for fear of litigation or blow-back. This is not exactly helpful to the school office team who work tirelessly and now have to cope with these legitimate requests. But rules are rules, and although this may seem cumbersome for a school, you can imagine what it feels like for a small, family-run business with 2-3 employees. It can sometimes feel like the good guys get penalised whilst the real outlaws continue to get away with it.

This process isn’t rocket science but can be tricky to implement and will cause you untold trouble if you do not have clear, easy-to-understand instructions for your customers (or parents) on how to request their ‘right’. If you’re unsure, the ICO has some great reference material.

In summary, we have 30 days in which to respond to these requests, and to ensure we uphold individuals’ data subject rights. But don’t forget, this includes keeping an accurate record of when the request was made, by whom, what amendment was changed (e.g. still like to receive marketing preferences on one specific brand but not the others), and of course, we all have to keep a record of when and how we managed the data subject request–so, ironically, no one is ever truly ‘forgotten’!

In summary, we have 30 days in which to respond to these requests, and to ensure we uphold individuals’ data subject rights. But don’t forget, this includes keeping an accurate record of when the request was made, by whom, what amendment was changed (e.g. still like to receive marketing preferences on one specific brand but not the others), and of course, we all have to keep a record of when and how we managed the data subject request–so, ironically, no one is ever truly ‘forgotten’!

In summary, we have 30 days in which to respond to these requests, and to ensure we uphold individuals’ data subject rights. But don’t forget, this includes keeping an accurate record of when the request was made, by whom, what amendment was changed (e.g. still like to receive marketing preferences on one specific brand but not the others), and of course, we all have to keep a record of when and how we managed the data subject request–so, ironically, no one is ever truly ‘forgotten’!

The Organisation relies on automated decision making or profiling only when appropriate

The Organisation has remediated identified high risk items and insured that transparent access to access policies are available to both customers and staff

Organisation staff are trained, and know how to recognise a subject access request and what to do with it

Organisation staff who process data subject rights requests have policy, processes and procedures in place to ensure processing without delay

Organisation systems are easily searchable, to identify where information is held

Organisation has policies in place to manage the creation and storage of information, so that it can identified and retrieved.

For a small, family-run business with 2-3 employees. It can sometimes feel like the good guys get penalised whilst the real outlaws continue to get away with it. The new rules mean that all changed under GDPR, the days of the Wild West data frontier were over. As we all wait, with bated breadth for the first organisation to be dragged over the coals, we’re all now aware that the real law was potentially worth it to some organisations, as the Regulator was pre-occupied with larger cases and any transgressions would have been punished with relatively minor fines.
THE MARRIOTT DATA BREACH is yet another example of poor data security where insufficient time and money has been spent on the most critical areas of data security and protection, so where does Cyber Security sit in the GDPR Maturity Framework?

Throughout my career, and like most CISOs and DPOs, I have always encouraged organisations to understand where their most critical data assets lie, how they flow from point A to B. Furthermore, I’ve always ensured that, depending upon the risk and vulnerability level, appropriate and proportionate risk-based controls are applied.

This includes ensuring that every point of ingress, every device and, ideally, every person has the suitable level of access control relevant to the role they perform. Of course, it’s easy to blame the systems administrator, or the unsuspecting user who innocently clicked on the phishing link, but the tough questions need to challenge how they were using the data: where was the data stored and who had access to it? Why was the data needed in the first place and when wasn’t used? And, of course, how do you keep checking that only the right people have access?

Only through answering these basic questions can you fully begin to appreciate how the data under your protection is being used, what technology or application is being used to deliver the functionality or services, what procedures sit behind the use, who needs access (and why) and critically, where and when is the data most vulnerable? Remember that these vulnerabilities change throughout the data’s lifecycle. Any decent risk assessment methodology will reveal what controls are needed and which controls will add the most value, but it doesn’t end there. A risk assessment, and subsequent penetration tests will inform the senior management where to focus efforts and deploy their cyber security experts, but it takes time, experience and knowledge about how systems and processes work, the people involved and the organisation’s culture. This has to be complemented by an awareness as to how these exploits are carried out, how likely they are to happen and how likely they are to materialise.

Article 32 does mention CIA but it’s also one of the shortest Articles and, inevitably, it leaves room for interpretation, and consider that the majority of cyber security breaches, litigation actions and fines are prosecuted under Article 32. When looking at this Article in particular, we should always bear in mind the potential for reputational damage, a drop in share price and losing the confidence of your stakeholders, staff and customers.

So why such little detail for such a fundamental issue? I suspect that the EU looked at the size of the $150 billion cyber security industry and assumed that there is sufficient expertise in the market; why would we hang our hat on one particular model? After all, one size does not fit all and there is no silver bullet.

Setting your red lines

When it comes to the security of personal data, my personal approach is to ensure that the CIA or Cyber Security function have a set of minimum ‘red lines’. These red lines come in many forms, but experience tells me that if you ask for too much you get very little, so I make sure that minimum red lines are achievable and—essentially—measurable and risk-based.

And that’s not forgetting every organisation’s biggest weakness—people training and awareness around risks such as phishing, tailgating, and forced wearing of badges. However, whilst we are busy working on the legacy data, don’t forget to mandate that all new projects, changes and upgrades to existing systems, processes, channels and data collection points are all subject to the Data Protection by Design review. The DPA should look at the project or solution and specify the ‘harm’ or ‘risk’ facing the individual or business should the appropriate privacy controls not be applied.

In many organisations, this relatively new process is still bedding down, so my advice is to at least ensure that you have defined your minimum red lines when it comes to data security and push your business and data owners to demand from Cyber Security how they are achieving these minimum best practices. On that note, please do not only rely on ISO27001 or other best practices to seek assurance that cyber security is working; instead challenge your team to prove to you how they are demonstrating compliance with your minimum rules.

In summary, the DPO and his/her team should be working hand-in-glove with Cyber Security (including Legal, Compliance, Risk and Internal Audits) to ensure that all the most appropriate risks and vulnerabilities are being adequately addressed, documented and managed. Whilst it might be tempting to leave Article 32 to the cyber security experts, I’m afraid you’ll be leaving yourself and the organisation potentially exposed unless you sit down with them and agree on these red lines.
NOW THAT YOU KNOW who owns the data, and you’ve put mechanisms in place to capture rights requests and report data breaches, surely ensuring that the workforce know what to do should be as easy as ‘one, two, three, e-learning’, right?

Wrong. Changing culture takes considerable time and effort, and the significance of this change should not be underestimated. Anyone who has spent time in the world of Cyber Security will know that persuading senior leaders to take the topic seriously is one thing, but, convincing them to lead by example and drive secure behaviour throughout their business operations whilst focusing on making a profit is quite another— but fundamentally this is what needs to be done.

After all, you are asking everyone who works for, and on behalf of, the organisation to be able to identify and report a data breach, and potentially oversignpost customers, suppliers, and employees to a rights request process. Both processes are time-bound, and, in the case of the data breach in particular, could have a significant impact on your organisation.

Getting The Message Across

I’ve seen some fantastic, hard-hitting awareness campaigns that have missed the mark because middle management simply didn’t have the time or, more importantly, were not tasked with making privacy or cyber security a priority. Unfortunately, this only becomes clear when an employee fails to spot a data breach or simply doesn’t know what to do with it.

I’m not saying that you shouldn’t introduce company-wide eLearning, or run awareness activities across every available channel to explain rights, breaches, and cyber security essentials. But what is absolutely essential is that you use all channels in your organisation relevant to each audience and you make sure that the people at the heart of the business—as well as those who have access to personal and company proprietary data—really know what is required of them. The only way to do this is to regularly test what you want them to know, make it very clear to the accountable owners what any shortfalls in knowledge will cost them and the business, and keep building on this. We’ll talk more about this in next week’s article on Demonstrating Compliance.

Empowering GDPR Champions

Ideally, once you have your accountable owners on board and on message, you will identify local data champions working across all areas of the business, focusing in particular on your high-risk areas to keep driving the messages home and testing that they work at the point of disruption. It is always advisable to regularly check-in with those working at the heart of the business; do they fully understand exactly what it is they need to do? How would they best remember this information? Just bear in mind that the answers may vary, depending on where and how they work.

Finally, don’t be afraid to ask for help from your internal communications and change management experts—these teams can be the key to ensuring that your training and awareness programme aligns to, rather than conflicts with, other company priorities; your programme should therefore be seen as an ongoing requirement, rather than a one-off project.

Victoria Guilloit has over 20 years’ cross-sector experience in the cyber security and privacy sectors. She designs and operationalises processes and is an expert in the field of Cultural Change. Vickie is our Awareness and Training Guru.

TOP TIP

Everyone loves free stuff. So, keep those vital awareness messages in constant view by putting them on pens and stationery, reusable coffee cups, or even mouse mats if people like them. Just not USB sticks— you need your CISO to support you too!

Desired State

- The organisation has appropriate data protection policies in place, and staff are adequately trained on them (and data protection in general), appropriate to their role. [Article 24 ]
- Appropriate data protection, records management and cyber security policies are in place.
- Senior Business Owner is responsible for the drafting and approval and communication of the policies, standards and guidance.
- Mandatory data protection training programmes established for all organisation staff/ contractors/ consultants/ secondees.
- Mandatory records management training programmes established for all organisation staff/ contractors/ consultants/ secondees.
- Specialist data protection training for senior management, or those accountable for data protection in the organisation.
- The organisation runs regular awareness campaigns.

Documents

- Records of training
- Awareness campaign material
- Role-based training material

AWARENESS CHECKLIST

- Role-based training material
- Awareness campaign material
- Records of training

Desired State

- The organisation has appropriate data protection policies in place, and staff are adequately trained on them (and data protection in general), appropriate to their role. [Article 24 ]
- Appropriate data protection, records management and cyber security policies are in place.
- Senior Business Owner is responsible for the drafting and approval and communication of the policies, standards and guidance.
- Mandatory data protection training programmes established for all organisation staff/ contractors/ consultants/ secondees.
- Mandatory records management training programmes established for all organisation staff/ contractors/ consultants/ secondees.
- Specialist data protection training for senior management, or those accountable for data protection in the organisation.
- The organisation runs regular awareness campaigns.

Documents

- Records of training
- Awareness campaign material
- Role-based training material

Desired State

- The organisation has appropriate data protection policies in place, and staff are adequately trained on them (and data protection in general), appropriate to their role. [Article 24 ]
- Appropriate data protection, records management and cyber security policies are in place.
- Senior Business Owner is responsible for the drafting and approval and communication of the policies, standards and guidance.
- Mandatory data protection training programmes established for all organisation staff/ contractors/ consultants/ secondees.
- Mandatory records management training programmes established for all organisation staff/ contractors/ consultants/ secondees.
- Specialist data protection training for senior management, or those accountable for data protection in the organisation.
- The organisation runs regular awareness campaigns.

Documents

- Records of training
- Awareness campaign material
- Role-based training material
What is compliance, why is it necessary and how can you achieve it?

Throughout the GDPR, the word “risk” is mentioned over 100 times. This is important because whenever you rely on risk to justify and mitigate a risk, you then need to be able to demonstrate that a control or safeguard specified is working and operational, in other words, that it is compliant. Additionally, whether you like it or not, demonstrating compliance is now a statutory requirement for every DPO or organisation that processes personal data (Article 37).

This also plays into the Accountability and Transparency principles (Article 5), where it is critical to assign ownership and responsibilities, whilst communicating to your customers and staff why and how you are using their personal data. This is typically contained within the Privacy Notice, and usually hosted on an organisation’s website. Such a document has to explain in clear and unambiguous language what, where, why, when and how contact can be made. This is crucial in demonstrating compliance and would be the first area where a regulator would initiate any investigations following a data complaint (Rights) or data breach (Cyber Security).

Accountability should promote and hold accountable how the data or risk owner is demonstrating that they are responsible. It is therefore critical to ensure you can show a regulator the internal ways of testing or validating that controls are being deployed effectively, that they have been tested and remain compliant with the laws and policies prescribed by your risk appetite.

Finally, compliance is necessary because we all need to be in a position that is defensible; should the regulator come in or should you find yourself unable to explain why certain risk-based decisions were made, and how they have been implemented or controlled (think audit) following a law suit or litigation case brought against you (think disgruntled employee or customer).

Compliance is another way of gaining peace of mind or providing assurance to your Board that the organisation is taking GDPR seriously and it is complying with the law. There is no simple way to achieve compliance, it is often manual, although there are many, many tools now available that can help you achieve your compliance goals.

The compliance goals or objectives is where you should start, don’t be tricked into buying a silver bullet. First, create a simple inventory of all your policy statements and legal provisions so you know what the differences are between ‘must’ and ‘should’ (e.g. the control framework). Once you’ve completed this you’ll have a better understanding of where the objectives will and can be met. Often we tend to think only about IT related controls, but there are many controls where people or process-oriented goals can be measured and tested; it’s worth thinking about these and gaining expert knowledge on them to see where they can feed into your control framework and be both measurable and demonstrable.

Compliance is a journey and, like any new framework or process, it takes time before it becomes second nature within an organisation. As with other global regulations, certifications and laws, the GDPR requires forms of testament that may or may not be applicable to your organisation, but you should have at least demonstrably considered why a provision is or isn’t measured.

---

**DEMONSTRATING COMPLIANCE CHECKLIST**

**Desired State**

- The organisation has appropriate levels of accountability which are understood at all appropriate staff levels.
- Data processing meets the legislative standard of ‘purpose limitation’, ‘data minimisation’, and ‘accuracy’ [Article 5]
- Personal data is processed by the organisation for no longer than is necessary for the purposes for which it was collected [Article 5, 1 (e)]
- Current, accurate, relevant and communicated privacy and/or cookie notices for all business processes
- The organisation’s Record of Processing Activities is accessible. [Article 30, Article 5 (2)]
- The organisation is taking GDPR seriously and is complying with the law. There is no simple way to achieve compliance, it is often manual, although there are many, many tools now available that can help you achieve your compliance goals.
- Compliance is another way of gaining peace of mind or providing assurance to your Board that the organisation is taking GDPR seriously and it is complying with the law. There is no simple way to achieve compliance, it is often manual, although there are many, many tools now available that can help you achieve your compliance goals.

16. GDPR Maturity Framework
Now let’s look at what we mean by ‘maturity’ across the five areas of Accountability, Rights, Cyber Security, Training & Awareness and Demonstrating Compliance.

Each of these five areas incorporates aspects of the twelve sub-domains that we have used to measure and compare ourselves against, across differing organisations and businesses.

Essentially, the GDPR Maturity Framework is a set of GDPR questions, split across these twelve critical domains, and they have been developed utilising the UK regulator’s ICO checklist, including Article 29 Working Party guidance, and EU EDPB notices, and all of the GDPR Articles and Recitals.

It is a practical interpretation of the GDPR text that takes into account the ‘how’ and ‘why’ a particular implementation or risk mitigation was selected.

It is not an audit framework, as the questions were developed in a way that would encourage the interviewee to be open and transparent in respect to their level of understanding, knowledge and accountability and does not rely on substantive evidence.

The maturity scoring (0-5) is also subjective and is based on the responses to the questions. It is however, a very good indicator as to how mature the procedures, documentation are that an organisation has in place, and can be used as a measure of GDPR maturity. The maturity rating has been developed using the internationally recognised Capability Maturity Matrix Integration (CMMI) developed by Carnegie Mellon University.

The following scores are applied to a respondent’s answers to deliver an overall maturity score:

- Optimal and independently verified: 4.5-5
- Managed controls and benchmarked: 4-4.5
- Managed controls but not benchmarked: 3-3.5
- Defined controls and fully implemented: 2.5-3
- Defined but not fully rolled-out: 2-2.5
- Repeatable controls: 1.5-2
- Ad hoc but some controls: 1-1.5
- Initial but ad hoc: 0.5-1
- Non existent: 0

The scoring is subjective and is based on the responses to the questions. It is however, a very good indicator as to how mature the procedures, documentation are that an organisation has in place, and can be used as a measure of GDPR maturity.
PrivacyCulture was created out of a desire to bring a real-world, human approach to the data privacy and cyber security sector—an industry dominated by large, faceless legal entities and the Big Four consultancies.

We pride ourselves on our ability to offer experienced, effective and personal solutions to businesses, departments and boards, regardless of size or sector.

We offer advice that is jargon-free, impartial and born out of decades of experience; we provide training that is based on hard-won knowledge; and we bring software solutions that are designed to be easy to use, comprehensive and measurable.

Fully utilising 50 years’ of combined working experience in implementing GDPR and delivering cyber security programmes, we have defined, refined and consolidated best practice to help your organisation ensure it is in a defensible position. We have built a repeatable GDPR Maturity Framework that allows an organisation of any size or structure to use the same five components to ensure a quality framework is in place and that this ‘defensible position’ can be measured in terms of its maturity.

Why not call us today and find out more about this revolutionary process and how it can be quickly and cost-effectively put to work in your business?