THE SUPPER CLUB


# BEYOND COMPLIANCE

Preparing for GDPR and a New Data Mindset

## About the authors

The Supper Club enables its community of fast growth entrepreneurs to make better, more timely decisions through curated peer learning. Members learn from each other in chaired roundtables and gain technical advice from experts in workshops and speaker events.

Edited insights from over 2,500 events are exclusively available to members through Learn Amp, a digital platform that allows businesses and communities to manage learning & development as well as track and report on compliance and risk management.

The Supper Club has produced this guide with Learn Amp to curate essential information about new data protection rules to help entrepreneurs prepare for GDPR compliance. It combines technical content sourced by Learn Amp with practical case study insight from members of The Supper Club and specialists in regulatory compliance.

While GDPR is a board level issue, it highlights a growing need for businesses to provide ongoing training to all staff about the risks associated with data processing and security to ensure true resilience and continuity.

Just as The Supper Club helps entrepreneurs to anticipate and manage a range of challenges related to scale, Learn Amp makes it easy and intuitive for individuals and businesses to access content and learning when and how they want and to track all activity in one place.

Thanks to all those who have contributed to this guide and shared their insight.

## Contents



## Contributors

# Introduction

**On 25th May 2018, General Data Protection Regulation (GDPR) will make businesses more accountable for respecting customer privacy and protecting their data. The consequences of incompetence and negligence could be fines of up to 4% of global turnover for breaches and potential for individual litigation.**

Yet, despite this potentially catastrophic threat to all businesses, many are still unprepared for GDPR (and not just in the UK). A Senzing study based on 1,000 senior executives from companies in the UK, France, Germany, Spain and Italy found that 60% are unprepared for GDPR.

A 2017 YouGov survey revealed that only 29% of UK businesses had started preparing for new data protection rules. This may be due to awareness, with 38% of those surveyed saying they were unaware of the new GDPR rules, and 33% thought it didn't apply to their sector. While 66% thought they could easily detect a data breach, only a third could report it within the 72-hour timescale set out by GDPR.

SMEs are only beginning to understand the full implications of GDPR. A survey of 1,003 SME owners by retail bank Aldermore last year found that just 9% had started preparing for GDPR and 46% hadn't even heard of it (that could represent 2.5 million of the UK's 5.5 million businesses).

**THE COST OF IGNORANCE**

This could mean a staggering amount in fines. A UK government survey in 2015 found that 90% of large organisations and 74% of SMEs reported a security breach, which led to an estimated total of £1.4bn in regulatory fines. Under new GDPR rules, with fines of up to €20m, UK businesses could face up to £122 billion in penalties (according to a report from the Payment Card Industry Security Standards Council in October 2016).

The threat of fines has woken businesses up to GDPR, and an industry has grown out of the need for compliance advice and services. There is an emormous amount of information about GDPR and from a range of sources, with many seeking to clarify GDPR.

But the Information Commissioner, Elizabeth Denham, has expressed concern about 'mis-information' and began a series of 'myth-busting blogs in August 2017. The first of these sought to play down the threat of fines and emphasise the core aim of GDPR to put customers and citizens first.

**Media, retail, construction, and manufacturing are the industries least well prepared for GDPR**

* UK Gov/Forrester (October 2017)

**33% of businesses don't think GDPR is an issue for their sector & 71% are unaware of fines they may face***

*YouGov (August 2017)

**On average, an EU company is set to get around 89 GDPR enquiries per-month after 25th May 2018 which could take up to 172 hours to complete***

*Senzing (January 2018)

**The three top concerns about GDPR* include:**
**- Unclear compliance steps**
**- Compliance needing a lot of user training**
**- Lack of understanding of the impact of GDPR by management**

*Spiceworks IT Snapshot (June 2017)

Organisations are beginning to embrace GDPR as an opportunity to build deeper trust and higher engagement with customers. They are looking beyond compliance to better manage client data and communication.

"The GDPR's emphasis on lean data management and resisting the magpie instinct to hoard customer data for its own sake impacts the heart of how customer engagement currently works," says Martin Hill-Wilson, Founder of Brainfood Consulting and chair of the Customer Data Security Directors Forum at Engage Infosec in January 2017.

"The GDPR enforces time out on this approach. It tells us we need to hand back the data once we have used it. If you have a value exchange mindset, then it's an opportunity to do your job and figure out what's next between you and the customer."

This point is echoed by Sam Clark, founder of Experience Travel Group and a member of The Supper Club who has spent the last year making his business compliant.

"The most positive thing about GDPR and the work we've done is reducing the amount of unnecessary communication because we want people to read our emails," he explains. "It's about the right message delivered at the right time in the right way, so it's worth the adjustment."

**A NEW DATA MINDSET**

A profound change of mindset about customer data is the real challenge and opportunity of GDPR for businesses.

While there are threats that business owners need to prepare for, GDPR is about investing time and resource in best practice that should deliver higher engagement and greater efficiency.

Our guide aims to clarify the essential points of compliance, help entrepreneurs understand the impact of GDPR on their businesses, what they need to do, and where they need specialist advice.

# GDPR: Past, Present & Future

**Data laws need to catch up with advances in mass communication to protect individuals.**

The last Data Protection Act was put into place in 1998, three years after 'Smartphone' became commonplace and nine years before the first iphone in 2007. With 20 billion smart devices predicted by the end of 2018, an update to this data law is long overdue.

But new data law must be robust enough for the next 20 years of change. A new Bill, published on 14 September 2017, aims to modernise data protection laws to ensure they are effective now and in the future.

The Data Protection Bill replicates GDPR, which has already been passed and has direct effect across all EU member states. However, GDPR does give member states limited opportunities to make provisions for how it applies in their country, so the Bill and GDPR should be read side by side.

Once passed, the Bill will help to clarify data regulations once the UK leaves the EU.

**ePRIVACY & GDPR**
While businesses have begun to understand GDPR compliance and its consequences, they will also need to consider ePrivacy and PECR.

Back in 2002, the EU ePrivacy Directive addressed the regulation of things like confidentiality of information, treatment of traffic data, spam and cookies. The Privacy and Electronic Communications Directive (PECR) is the UK-interpretation of ePrivacy. In 2009, ePrivacy was amended with some key changes, most notably making cookies subject to prior consent.

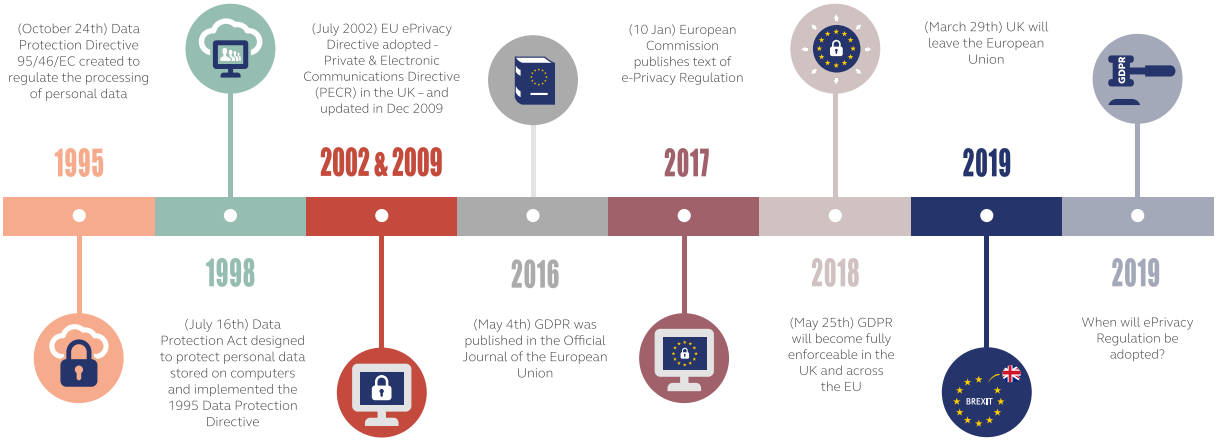
In January 2017, ePrivacy Regulation was published to update the ePrivacy Directive. It encompasses all definitions of privacy and data introduced within the GDPR; but it also clarifies and enhances it in areas such as unsolicited marketing, cookies and confidentiality.

**PROTECTING PRIVATE LIFE AND DATA**
GDPR and ePrivacy Regulation were both drawn up to reflect different parts of EU law and the European Charter of Human Rights.

GDPR was created to protect personal data, while ePrivacy relates to a person's private life. GDPR is updating and unifying European data protection laws, and ePrivacy reform is doing the same for electronic communication and marketing laws, replacing country-specific legislation with a new European regulation.

While it was hoped that ePrivacy Regulation would be adopted alongside GDPR on 25th May 2018, it is now expected in 2019.

## Data Protection, GDPR & ePrivacy Regulation Timeline



## Commissioner Insight: GDPR Myths

**Elizabeth Denham, the UK's Information Commissioner, began a series of blogs in August 2017 designed to address some of the confusion and 'scaremongering' related to GDPR and how it will be enforced by the ICO. Below are five of the 'myths' she highlighted with some of her clarifying comments:**

**'The biggest threat to organisations from the GDPR is massive fines'**

*"This law is not about fines. It's about putting the consumer and citizen first. We can't lose sight of that … It's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm."*

*"The ICO's commitment to guiding, advising, and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick. Issuing fines has always been and will continue to be, a last resort. Last year (2016/2017) we concluded 17,300 cases. I can tell you that 16 of them resulted in fines for the organisations concerned."*

*"Like the DPA, the GDPR gives us a suite of sanctions to help organisations comply – warnings, reprimands, corrective orders. While these will not hit organisations in the pocket – their reputations will suffer a significant blow."*

**'You must have consent if you want to process personal data'**

*"The new law provides five other ways of processing data that may be more appropriate than consent. 'Legitimate interests' is one of them and we recognise that organisations want more information about it. There is already guidance about legitimate interests under the current law on the ICO website and from the Article 29 Working Party. We're working to publish guidance on it next year … But there's no need to wait for that guidance.*

*"You know your organisation best and should be able to identify your purposes for processing personal information."*

**'All personal data breaches will need to be reported to the ICO'**

*"It will be mandatory to report a personal data breach under the GDPR if it's likely to result in a risk to people's rights and freedoms. So if it's unlikely that there's a risk to people's rights and freedoms from the breach, you don't need to report."*

**'All details need to be provided as soon as a personal data breach occurs'**

*"Under the GDPR there is a requirement for organisations to report a personal data breach that affects people's rights and freedoms, without undue delay and, where feasible, not later than 72 hours after having become aware of it."*

**'GDPR compliance is focused on a fixed point in time – it's like the Y2K Millennium Bug'**

*"GDPR compliance will be an ongoing journey. Unlike planning for the Y2K deadline, GDPR preparation doesn't end on 25th May 2018 – it requires ongoing effort.*

*"That said, there will be no 'grace' period – there has been two years to prepare and we will be regulating from this date. Those who self-report, who engage with us to resolve issues and who can demonstrate effective accountability arrangements can expect this to be taken into account when we consider any regulatory action."*

**USEFUL LINKS:**

**GDPR searchable by chapter and provision:** https://gdpr-info.eu/

**ICO's checklist and guidelines on GDPR:** https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/principles/

**ICO small business GDPR helpline (0303 123 1113, option 4) and live chat:** **https://ico.org.uk/global/contact-us/live-chat/**

## Impact of GDPR on fines

**Using the current maximum penalty as a guide, NCC Group created a model to determine what tier the fine would fall into and what a maximum post-GDPR fine would likely be. The table below highlights two high profile corporate and SME examples:**

| Company | Fine/Year | Equivalent fine post-GDPR* |
|---|---|---|
| Pharmacy2U | £130,000 (2015) | £4.4m |
| Talk Talk | £400,000 (2016) | £59m |

**Calculated by NCC Group 2017*

# Understanding New Data Risks

**There are a range of new data risks to mitigate under GDPR, from breaches of consent and cyber security to reputational damage and personal damages claims from individuals.**

The key risk you need to prepare for is someone asking where you got their data from; so you need to know, and you need to be able to recall the information easily to be able to respond quickly.

Individuals can claim damages without the need to show any evidence of harm to support their claim; but you can make your business less of a target for PPI-like claims by documenting everything to prove you have tried your best to prevent a breach.

You will need to notify the ICO and the individual concerned about a breach within 72 hours, so you will need someone in your team who is responsible for managing this promptly.

**PRIVACY ACTIVISM**

With 5.5 million businesses in the UK, some have questioned whether the ICO has the resources to police compliance for all of them; but there are others who may scrutinise your business for data breaches.

A disgruntled customer or former employee might post something on social media that leads to hundreds of requests for personal data at once. While they must all provide proof of ID, you must be able to respond to these requests within 30 days.

Consumer groups or privacy activists may target you, particularly if you process or monitor a substantial volume of personal data. Competitors might attempt to damage your reputation by challenging how you process data or obtained consent.

To protect your business from new data related risks you may need to appoint, contract, or train someone to build and manage new processes and systems.

**PROTECTION FROM FINES**

While an investment in compliance might seem expensive to SMEs, it must be weighed against the prospect of incurring substantial fines under GDPR or damage to reputation following an audit. Currently, the ICO can apply fines of up to £500,000 for contravening the Data Protection Act 1998.

Once GDPR comes into force on 25th May 2018, a two-tier system will apply: lesser incidents will be subject to a maximum fine of either €10 million (£7.9 million) or 2% of global turnover (whichever is greater). The most serious violations could result in fines of up to €20 million (£17 million) or or 4% of turnover (whichever is larger).

# GDPR Glossary: Key terms and acronyms related to new regulation

- **Breach.** A breach means any breach of the law, not just a breach of security or a hack. The larger fines are reserved for things like a breach of consent rather than security (where the fine is half of this).

- **Consent.** Under GDPR, consent means 'the individual's freely given, specific, informed and unambiguous indication, either by a statement or by a clear affirmative action, signifying their agreement to their personal data being processed'

- **Data processors & controllers.** Processing is defined as any operation performed on personal data, such as storing, collecting, recording, organising, sharing, or deleting. A controller is also a data processor, but they also decide the purpose of processing. For example, if you use a CRM system you are the controller. The third-party provider of the CRM system is the processor.

- **Data Protection Officer.** The primary role of a DPO is to ensure everyone in an organisation is fully compliant with all GDPR legislation.

- **Double opt-in.** Verifying that an email address is active and the details are correct is referred to as 'double opt-in'. The process means that when a data collection form is submitted an automated email is sent and the new subscriber data is only confirmed and added to the database once a verification link has been clicked.

- **Encryption.** The process of converting information or data into a code, especially to prevent unauthorized access

- **Entity resolution and analysis.** ER&A is a process that helps administrators to gather a complete body of data about a particular individual from different information siloes.

- **ePrivacy Regulation.** This broadens the scope of the current ePrivacy Directive, aligns the various online privacy rules across EU member states, and enshrines the protection of a person's private life alongside GDPR protection of personal data.

- **General Data Processing Agreement (GDPA).** Designed for the transfer of data between entities inside and outside the EU, this is a legal document signed and adopted by all companies within a group, which sets out how they all agree to secure and protect personal data they share.

- **Information Commissioners Office (ICO).** The ICO enforces data legislation and can issue fines for breaches of GDPR.

- **Legitimate interest.** For marketing purposes, Legitimate Interest must be genuine and based on a relevant and appropriate relationship. According to the DMA, 'marketers must weigh up their right as a business to market to someone against the individual's right to privacy; they must offer a clear opt-out and have a compelling case for why someone might be interested in their goods or services'.

- **Privacy by design.** This is a new approach that promotes privacy and data protection compliance from the start; for example, yes or no options and no default selections.

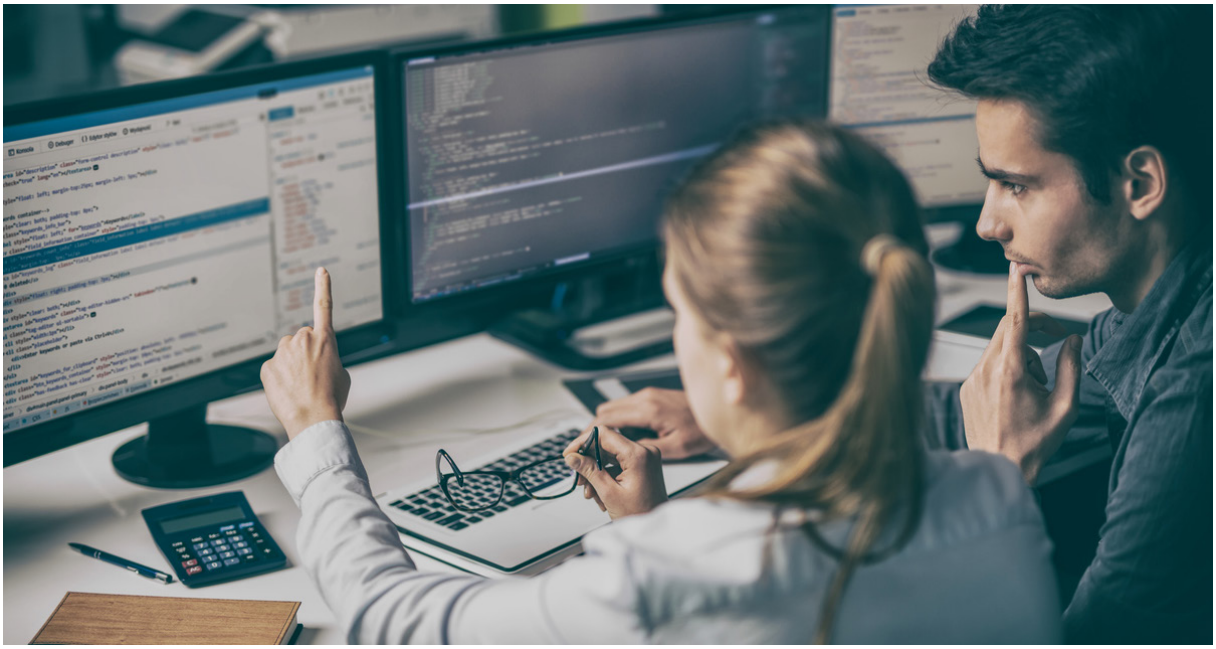
- **Privacy Shield.** Privacy Shield is an agreement allowing for the transfer of personal data from the EU to US. It is designed to meet the requirements of GDPR regarding the transfer of data out of the EU whereby participating companies are deemed as having adequate protection.

- **Privacy and Electronic Communications Regulations.** PECR sits alongside the Data Protection Act and gives people specific privacy rights in relation to electronic communications.

- **Personal Identifiable Information.** PII underpins GDPR and applies to both B2B and B2C uses including email address, mobile phone number, bank account details, address, credit card number, driver/passport number, genetic or biometric data.

- **Pseudonymization.** This means separating personally-identifiable information from other data attributes to avoid security risks.

- **Subject Access Requests.** SARs are the means by which an individual can either request to see all data held on them, or request that all their data be deleted. It must be supplied in a portable, machine readable format within 30 days.



## Guide to GDPR compliance

**Based on the ICO's 12-steps to becoming GDPR compliant, here is a practical guide to what you need to do with curated tips on how to do it**

*"GDPR is not an IT issue, it's a business wide issue. It should be the MD's responsibility with some external help to make sure people are going in the right direction; but the whole board need to step up and take ownership of their particular part of GDPR."*

**Steve Clarke, Co-founder, Freeman Clarke**

## 1. Awareness

**The first and most urgent step in preparing your business for GDPR is awareness, so you will need to ensure everyone in the organisation understands GDPR and its impact.**

The board is ultimately responsible for GDPR compliance and must ensure it is properly resourced, monitored and reported on. It may be necessary to appoint a Data Protection Officer (DPO) to manage compliance, or train someone in the team to take on this role, but they must be able to drive this through the business and report to the board.

| Action | Challenge | Solution |
|---|---|---|
| Make GDPR part of your board reporting on your risk register and ensure someone is monitoring and managing threats | Who will manage the process for compiling a list of threats, monitoring them and reporting to the board? | Recruit a DPO or appoint an existing employee, train them, and put procedures in place |
| Create a culture of compliance by making GDPR part of the induction for new joiners and regularly remind the team about its key requirements in refresher sessions | How do you deliver GDPR training in a way that is easy to recall and implement? | Be specific and tailor training for each job role using working examples of where a breach could occur and how to be compliant in that situation. Platforms like Learn Amp can promote awareness of GDPR related issues online, as well as track and test understanding |

## Member Insight: Getting Compliant

**Sam Clark Co-founded Experience Travel Group in 2006 to provide authentic holidays in Asia for travellers looking to combine luxury and adventure. It has been updating systems over the last 12 months in anticipation of new data regulation.**

**When did you start working on GDPR compliance and why?**

Our part time IT director flagged it on our risk register a year ago and said it was something we needed to get on top of. We're a consumer business so I was most worried about having a lot of customer data that we might not be able to make compliant, so it could shrink our marketing list.

**How did you start the process?**

It began with fact-finding to get a clearer picture. Me and different members of the board attended a few seminars, and we learned a lot from a series run by TravLaw in association with our trade industry body, AITO. They took quite a bullish view on GDPR, advising that we should be OK if we are compliant with the most recent Data Protection Act and a stricter reading of GDPR will need to be tested in court.

**What were your main priorities and how did you address them?**

**Sam Clark, Co-founder of Experience Travel Group**

Email marketing is a big focus as our customers need to be signed up to the right thing at the right time for different stages of need. It's been very complicated; we worked with Hubspot. It was less about GDPR compliance and more about needing to adapt our messaging and email system for clients; but if we're challenged we can demonstrate that it's compliant and we have all the due diligence.

The other part of the process we're looking at now is who will manage data protection. We are getting someone in to get our house in order and create processes that will become part of the marketing function. We'll be adding it as a board item as part of our risk profiling to ensure someone is on it and we're all up to date.

**What are you still working on or trying to clarify?**

We're still not clear on when we need to go with a double opt in to receiving communications. It's double or nothing with our platform so a big step that we need to be clear on.

**Have there been any unexpected benefits from the process?**

Ultimately, we want our emails to be read so if we and everyone else are sending fewer emails it's better for everyone. We will be better at sending the right message at the right time in the right format so it's worth the adjustment.

## 2. Storing Information

**GDPR is updating rights for a more networked world and the risk of sharing inaccurate personal information with other organisations. It requires you to maintain records of your processing activities, so an information audit across your business will ensure you know exactly what personal data you hold, where it came from, and who you share it with.**

To avoid being impacted by any breaches outside your control, it's recommended that you conduct due-diligence on your supply chain. Check obligations in contracts to ensure your suppliers and contractors are GDPR-compliant.

Review your purchased data, ask the supplier how they gathered it, and what permissions they have, and ensure you record and document this. Review your web host if data is moving between operations in different countries.

Check your suppliers and any systems that store your customer data to confirm where it's hosted. Document everything to have a clear record that you can produce upon request.

**HISTORICAL DATA**
There is some ambiguity around historical data in terms of how long consent is valid and how long it can be justifiably held.

Some experts believe that, as long as it can be proved that measures and processes were in place to capture explicit consent, then it can be held after 25th May without having to regain consent.

After GDPR, privacy policies must clearly state how long data is held and for what purposes.

The length of time that personal data can be justifiably stored will be based on the legal grounds for storing it. There are statutory requirements on storing financial data for at least seven years, but customer data is based on sales cycle which is usually 12 months.

The GDPR deadline is an opportunity to clean out your databases and ensure your marketing is targeting only engaged individuals. If your database hasn't interacted with you or responded to your marketing within 12 months, it's generally recommended that you do not communicate with them anymore.

If you are running campaigns to re-engage individuals before 25th May 2018, be aware that they may withdraw their consent.

Under GDPR there will be stricter rules on incentives for gaining consent and opt-out or unsubscribe options must be clear and easy to use in these communications.

| Action | Challenge | Solution |
|---|---|---|
| Segment your email data into anyone who has opened an email in the last 12 months or within your justifiable and reasonable sales cycle | Organisations often have several contact lists for different types of email comms and the same individual could be on multiple lists. They may be engaging with one type of comm but not another, so how do you segment them? | If your email system supports advanced query building, you should be able to segment unengaged subscribers across all types of communication and remove as a group |
| If you're getting close to the 12-month mark since they last engaged, try to re-connect; but opt-out or unsubscribe options must be clearly on communications | The unsubscribe option is often associated with a specific communication type, so a recipient might think they're unsubscribing from all communication | Build a preference centre on your email system, so clicking unsubscribe allows them to see all communication lists they've signed up to and choose which they'd like to be removed from |

## Expert Insight: Storing Data

**Peter Borner is an entrepreneur with senior leadership roles with global firms including Sony Music and British Telecom. Peter answers some key questions about storing data with insights from helping small and large businesses mitigate the risks of compliance.**

**Of the firms that you've reviewed, where are the more obvious failings, and does it depend on size of business or sector?**

Most I have reviewed have started far too late. The GDPR was brought into law in April 2016 and they are only just waking up to the fact that the end of the transition period is approaching fast. Small firms tend to believe they are not affected because they have largely ignored the Data Protection Act for the last 20 years; but the publicity around GDPR will ensure that data subjects know more about their rights.

For larger firms, I have found a lack of understanding that consent between employee and employer is contentious; because it's difficult to prove that consent can be freely given by an employee. Firms need to find other legal grounds for processing employee data other than consent. This means they must change their approach or they will create an issue going forward.

**Under GDPR, must data be stored in the EU and what if servers are in the US?**

Data does not need to be stored in the EU and it can be stored in the US. However, sufficient safeguards must be in place when transferring data out of the EU. We recommend a General Data Processing Agreement (GDPA) between entities inside and outside the EU. This is a legal document signed and adopted by all companies within a group, which sets out how they all agree to secure and protect personal data they share.

If you cannot get a GDPA then you have to rely on standard clauses (as defined in the GDPR). AWS and Microsoft rely on the standard clauses. Simply relying on the US Privacy Shield is not sufficient. All transfers to third countries will have to be correctly and fully documented in your Article 30 records.

**Peter Borner, Senior Consultant, The GDPR Guys**

Google and Microsoft have put in place the standard clauses and updated their Data Privacy notices to be GDPR compliant.

An interesting point recently came up about the use of DropBox. Using the Plus individual edition that lots of SME and startups choose allows you to generate a shared link to a file or folder that, when used, requires no authentication to access the data. So, not only do we not know where in the USA Dropbox stores your data, it is possible for an employee to accidentally cause a breach.

**What is considered a reasonable length of time to keep personal data and how can this be justified?**

Data can only be stored for as long have you have legal grounds for storing it. Financial data often has to be stored for 7 to 10 years. Employee data needs to be stored for as long as you need it to defend yourself against industrial tribunals. Customer data is generally stored for the length of your normal sales cycle. It is a case by case decision. The implications of this are that you may be able to refuse a request for erasure because you have the legal grounds for keeping the data for longer.

## 3. Communicating Privacy

**Privacy notices are important because customers and employees will be more aware of the value of their data and will expect you to be clear and open about why you are collecting it.**

In addition to who you are and how you intend to use their data, you will need to explain the lawful basis for using it, how long you will keep it, and their individual rights to complain if they think there is a problem with how you handle it. Privacy notices will need to contain the following information:

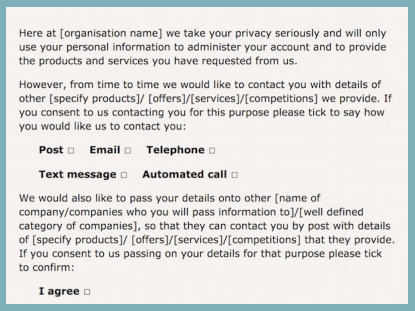
- **Who you are** – it needs to be clear who is controlling the data
- **What you are going to do with their data** – you need to explain the purpose for processing personal information and the legal basis for doing so
- **Who it will be shared with** - you need to specify who and why

One of the challenges related to privacy notices under GDPR is that they need to be concise, transparent and written in language a child can understand but may need to include a lot of information to be compliant. Using links or layering is a solution suggested by the ICO (see **Example Privacy Notices**).

| Action | Challenge | Solution |
|---|---|---|
| Ensure privacy notices are clear and in layman's terms, and you have the right consents for how you plan to use data | Who in the organisation understands both digital and offline data capture policies and data flow, storage, and usage processes; and can rewrite privacy notices for all channels? | Create a working group of individuals across relevant teams who could feed into this. Work with a GDPR consultant to review existing processes and rewrite privacy policies |
| If your customers haven't consented under GDPR resend your updated privacy policy and ask for consent | If they do not respond or do not give consent this could significantly reduce your data list | For existing customers and those in negotiation, consider 'soft opt-in' with a clear opt-out message (see **GDPR, PECR & ePrivacy** on pg 15) |
| If you are going to do different things with customer data, get consent for each use | Does your email system allow you to build a preference centre where contacts can manage their communication preferences? | If so, use it to get consent from existing customers. Give a heads-up call followed up with email. If not, use a simple form builder tool to capture consent and manually update contact records. |

## Example privacy notices

The ICO has provided some examples of privacy notices at https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/what-should-you-include-in-your-privacy-notice/
Privacy notices should clearly and simply explain what will be done with personal data, by whom, and who it will be shared with. 'Layering' users to access easy-to-understand information and then delve more deeply if required…



Here at [organisation name] we take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us.

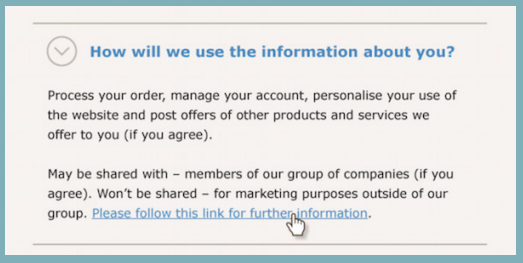
However, from time to time we would like to contact you with details of other [specify products]/ [offers]/[services]/[competitions] we provide. If you consent to us contacting you for this purpose please tick to say how you would like us to contact you:

**Post** □ **Email** □ **Telephone** □

**Text message** □ **Automated call** □

We would also like to pass your details onto other [name of company/companies who you will pass information to]/[well defined category of companies], so that they can contact you by post with details of [specify products]/ [offers]/[services]/[competitions] that they provide. If you consent to us passing on your details for that purpose please tick to confirm:

**I agree** □



**How will we use the information about you?**

Process your order, manage your account, personalise your use of the website and post offers of other products and services we offer to you (if you agree).

May be shared with – members of our group of companies (if you agree). Won't be shared – for marketing purposes outside of our group. Please follow this link for further information.

## 4. Individual's Rights

**The right to be forgotten has grown out of the rise of social media and more personal information being published online.**

This is based on concern about the potential stigma of things said or done in the past that may impact one's future.

The EU is introducing a limited 'right to erasure' as part of GDPR compliance. This means that any EU citizen can request that data held about them is erased if: they had to give consent for data processing and now choose to withdraw it; there is no longer a reason for the data to be processed; the data was collected or processed unlawfully; or another legal obligation requires the data to be erased.

Whether you hold records in a spreadsheet or a CRM system like Salesforce, it's important to prepare for proof of deletion or proof that a record is held in a suppression list (ie where opt-out emails are stored).

## 5. Subject Access Requests

**Under GDPR, anyone can ask you for a full report of what data is kept on them. It's called a Subject Access Request (SAR) and you will have 30 days to provide the data.**

If you can't provide it in 30 days, you will have to request an extension for up to 2 months. If you can't ever provide it, you must clearly state why not.

While SARs aren't new, they have been subject to payment of a nominal fee. Under GDPR, they will be free.

Businesses should be preparing for SARs from customers and prospects who have received communications. Employees past and present can also request access to their personal information. Both must have a legitimate reason to ask for this data and they must provide proof of ID.

You can challenge a request for access, but always take it seriously and always ask them to verify their identity.

Smaller companies face one or two key challenges around retrieving customer data. Firstly, it is often spread over various network folders, databases, and individual terminals.

This could be costly. In its January 2018 survey, Senzing found that firms with 10+ employees will have almost 20 hours a day of extra work and SMEs will need someone to dedicate an eighth of their day to retrieve relevant customer data from disparate databases (see The Data Collection Challenge).

Secondly, smaller businesses often rely on third party data handlers that store and process customer data, so they are deemed as data processors under GDPR.

Upon request, your data controllers must be able to confirm whether they process an individual's personal data and provide a machine-readable copy of it so that they can send it to another provider if they wish.

## 6. Processing Personal Data

**There are six lawful bases for processing data under GDPR and at least one of them must apply.**

The first is consent, where an individual has clearly agreed that their personal data can be processed for a specific purpose. The others include:

- **Contractual purposes** – as part of a contract or steps taken before entering one
- **Legal obligation** – to comply with the law (not including contractual obligations)
- **Vital interest -** which is necessary to protect someone's life
- **Public interest** – to perform a task or official function with a clear basis in law
- **Legitimate interest** – for direct marketing, security, or internal administration

The ICO states that businesses must not adopt a one-size-fits-all approach and no one basis should be seen as always better, safer or more important than the others. Deciding which lawful basis applies will depend on your specific purposes and the context of processing. You will need to make this clear in your privacy notice.

Consent and Legitimate Interest are the most nuanced and the ICO has been working with the Direct Marketing Association (DMA) to provide further guidance.

| Action | Challenge | Solution |
|---|---|---|
| Prepare for a deletion request by auditing all data you hold & define your justification for holding it | Data is usually held in shared and individual mailboxes, deep in folders on shared hard drives, or in cloud storage | Contract staff to search all storage to find this data. If it's not being used on a CRM/email marketing platform, delete it |
| Define your process for dealing with any requests and responding within 30 days (may need to notify other businesses if you've passed on someone's data) | What if I'm trolled in a concerted attack by individuals or groups requesting their personal data all at the same time? | You can extend the deadline by 2 months if requests are sufficiently excessive or complex but notify the individual within 30 days and explain the extension |
| Review and clarify contracts with any service providers and their processes for handling customer requests. | Who can identify potential loopholes in your organisation and what can you do if they are found in a service provider's processes? | Get a GDPR consultant or trained and qualified member of the team to review these contracts |
| Carry out a data audit of customer and employee data, assess related processing activities and identify any GDPR gaps | There may be gaps in knowledge if people have left your organisation | Bring staff together to break it down and cover more ground more thoroughly; document as you go along, identifying opportunities to optimise processes and fill any gaps |
| Review and update privacy notices as all information provided must be easy to understand for customers, employees, and job applicants | Who has the skill and understanding to apply all changes to re-write privacy policies? | You may need to hire a specialist consultant to train someone in your team |

## The Data Collection Challenge

| | Average enquiries per month | Average number of databases | Average minutes per enquiry | Total minutes per month | Total hours per working day |
|---|---|---|---|---|---|
| **All** | 89 | 23 | 5 minutes, 2 seconds | 10,317 | 8 hours, 11 minutes |
| **Large** | 246 | 43 | 7 minutes, 8 seconds | 75,527 | 59 hours, 56 minutes |
| **SME** | 15 | 18 | 4 minutes, 58 seconds | 1,339 | 1 hour, 3 minutes |
| **Micro** | 7 | 9 | 3 minutes, 2 seconds | 191 | 9 minutes |

** Senzing Survey January 2018, calculating the total quantum of time per month that a company will have to spend solely searching its databases from a survey of executives*

# 7. Consent

**Until now, businesses only had to ask consent once to cover all uses. Under GDPR, businesses will need separate permission for each different use of data.**

Consent must also be freely given (a genuine choice without detriment or loss of service), informed (information must be specific and unambiguous), clearly agreed (pre-ticked boxes, silence or inactivity don't constitute consent), and proven (documented, dated and how you gained consent).

Under current data protection regulations, you need consent or an existing customer relationship to send email marketing.

"If you want to make your emails more timely, targeted and tailored to the individual, you need data: demographics, preference, purchases, browsing behaviour, location and device information," explains Steve Henderson, Communicator Compliance Officer and chairing of a GDPR Hub Group at the Direct Marketing Association (DMA).

"All this extra information can help make email more relevant and valuable but data protection regulations (DPA and GDPR) require you to have a legal basis for this. This is to ensure what you do is fair, transparent, not excessive, and to make sure you look after the data you collect, store and use. And for that you need consent or 'legitimate interest'."

But GDPR requires that you explain all of your intended uses of data and the legal bases for processing it in full before you collect it. If you want to run different campaigns in the future, or add new content to communications, you need specific permission before you collect data. And you need to do this in a way that makes your customer want to sign up to it before they benefit from your product or service.

Steve Henderson suggests that Legitimate Interest might be easier. "You still need to explain and give relevant choices and appropriate control over what you do; but you have a little more flexibility over how you give this information because you can explain about the new data use when you start using it."

The DMA has produced guidance on using Legitimate Interest (LI). It says the interests of an organisation must not outweigh the privacy rights of individuals. Marketers must offer a clear opt-out and have a compelling case for why someone might be interested in their goods or services.

**LEGITIMATE INTEREST ASSESSMENT**

The ICO's guidance on deciding if there is a legal basis for processing is to undertake a Legitimate Interest Assessment. This is a three-part test based on three questions:

- **Purpose test:** are you pursuing a legitimate interest?
- **Necessity test:** is the processing necessary for that purpose?
- **Balancing test:** do the individual's interests override the legitimate interest?

GDPR states that 'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.'

"Right now, it's OK to use LI when direct marketing provided you give data subjects the ability to withdraw consent," says Peter Borner of The GDPR Guys. "If you have an existing and engaged customer, you may be able to use other legal grounds such as performance of a contract.

The key with LI is create a defensible position, adds Borner. "A firm should be careful to record their reasoning. If you feel you can justify LI you are probably in a good position should the ICO come knocking. If the ICO disagrees you should be prepared to listen and update your approach.

"The ICO are a reasonable organisation and will go after those firms that are either blatantly ignoring or subverting the regulation. You may end up with a letter of enforcement, but it is hardly likely to result in a fine unless you then decide to ignore the ICO's letter."

**LI & EMPLOYEES**

Consent isn't only an issue for new and existing customers, it also applies to employees.

"Currently, employers can justify processing personal data on the basis of employee consent; but there is doubt as to whether or not consent is given freely in the employer-employee relationship," says Ally Maughan, CEO of People Puzzles and a member of The Supper Club. "GDPR will make it harder for employers to rely on consent to justify processing."

Some legal experts have warned that individuals may use their rights - where data has been processed on the basis of consent -

as a tactic to stall disciplinary or redundancy processes.

Employers will need to look at each of the purposes for which it processes employee personal data then document the lawful grounds under the GDPR relevant to each. This should cover contract performance for employee salary payments, with Legitimate Interest for processing connected with monitoring performance, discipline, and employment law requirements (see CONSENT IN EMPLPOYMENT CONTRACTS).

**LEGITIMATE INTEREST IN PRACTICE**
**Here is an example email from the DMA...**

Thank you for buying with us.

We believe that based on your purchase you would be interested on other related cloud computing solutions we offer. We will send you emails about our products and services and look forward to doing business with you again soon.

If you wish to not receive marketing from us then please click here and you will instantly be unsubscribed from our email database.

We have prepared a plain English and simple privacy policy that explains how we will use your personal data. Follow the link to find out more.


**CONSENT IN EMPLOYMENT CONTRACTS**
**To help employers prepare for changes under GDPR, here are some recommendations from Olivia Sinfield, Associate Director at law firm Osborne Clarke:**

- **Conduct data mapping:** Establish what data is processed, why and for how long and then consider which of the legal grounds for processing apply to each data type (avoiding, where possible, consent for reasons set out below). For example, are certain types of processing a contractual necessity (such as employee payment data), required to enable the employer to comply with a legal obligation (such as social security data) or in the employer's legitimate interests (where an assessment has been made that those interests are not overridden by the potential harm to the individual)?

- **Reconsider the use of standard consent clauses in employment contracts:** The use of generic clauses in employment contracts which seek to obtain broad consent from the employee to processing of their personal data will not be valid. This is because such consent is not 'freely given' due to the imbalance of power in the employment relationship. Such clauses should not be used in contracts of employment going forwards but, instead, employees should be notified via a Privacy Notice of the alternative grounds for processing of personal data.

- **Amend your contract of employment template:** Your contracts should include a re-written data protection clause making compliance with employee obligations in respect of data processing a term of the contract and specifying that breach may result in disciplinary action being taken, up to and including summary dismissal. Employees should be directed to their obligations as set out in the employee Privacy Notice and a Data Protection and Information Handling Policy.

- **Amend or re-write your Privacy Notice and Data Protection and Information Handing policy:** To meet the mandatory requirements of the GDPR and to include the alternative grounds relied upon for processing of personal data.

- **Separate declaration:** Where consent remains necessary then a new approach to consent is crucial (in very limited circumstances and mainly in relation to special categories of data where processing is not justified on the grounds that it is necessary for the purposes of performing or exercising obligations or rights in the field of employment law).

Consent provisions must be included in a separate declaration which is not intrinsically linked to the employee's acceptance of employment. The declaration must be detailed, specific and explicit as to its purpose and should be tailored to each business. There should also be a mechanism in place (in your back-end systems) to enable an employee to withdraw consent at any time and with no detrimental consequences.

- **Communicate changes:** Forward plan your internal process for communicating with employees about these changes to their employment contracts and how information will be made available to them via new Privacy Notices and the Data Protection and Information Handling Policy.

# Expert Insight: GDPR, PECR & ePrivacy

**Steve Henderson is Compliance Officer at Communicator and chair of a group working within the DMA to develop practical guidance on email marketing under GDPR. He explains the differences between GDPR, PECR and the ePrivacy Directive and what this means for marketing consent.**

A Google search for "GDPR and email marketing" brings 138,000 hits. This is interesting because in the GDPR, "marketing" is mentioned four times and "email" is mentioned once. While the GDPR governs the data you use for email marketing, the required permission to send email marketing is defined by PECR.

ePrivacy is a European directive. PECR is the UK-interpretation of ePrivacy. In the same way that the GDPR is updating and unifying European data protection laws, ePrivacy reform is doing the same for electronic communication and marketing laws, replacing country-specific laws with a new European regulation.

'PECR' defines the means of gaining permission to send email marketing. It's quite simple, as there's only two: with consent, and to existing customers or those in negotiation for a sale or service.

## GDPR & EMAIL MARKETING WITH CONSENT

GDPR isn't just changing the standard of consent for data processing, but it's also changing the definition and standards for consent. Because that definition is used by PECR, the GDPR is indirectly changing the consent requirements for email marketing.

To make sure existing consent-based marketing lists are GDPR compliant, review your record keeping. You'll need to re-permission your data where you can't show where and when someone gave consent or what they gave consent for.

## SOFT OPT-IN

Consent is not the only means of gaining permission for email marketing. PECR also allows email marketing, in certain circumstances, to existing customers and those in negotiations for a sale or service. Those circumstances are: where the email address was provided during the sale or negotiation process; where an option to opt-out was provided; where the marketing is limited to goods and services relating to the purchases or customer relationship; and where the customer is given an option to opt-out in each message. This situation is sometimes referred to a "soft opt-in".

**Steve Henderson, Compliance Officer, Communicator**

To make sure existing customer marketing lists are GDPR compliant, you'll need to show that these recipients are actually customers and show that the sign-up information and marketing opt-out was clear and simple to understand. You'll need to re-permission your data where you can't show the customer status or ongoing marketing permission.

## EMAIL MARKETING & LEGITIMATE INTEREST

Nowhere in PECR does it list "legitimate interests" as a legal basis for sending electronic marketing, but the GDPR does allow some "processing for direct marketing purposes" under legitimate interests. This isn't a contradiction: "processing" includes so much more than actually sending marketing. For example, you may use personal data for profiling, targeting and segmentation. These enhancements to your marketing are examples of processing data for direct marketing purposes where you may be able to use legitimate interests.

For all the personal data you collect and use for your marketing the transparency and fairness of use provisions of the GDPR apply in full.

The legal basis for email marketing hasn't been materially changed by GDPR. Email marketers need to understand both GDPR and PECR.

PECR allows email marketing with consent, or where there is a customer relationship. Where email marketing is on the basis of that customer relationship it can be on an opt-out basis, but the marketing must be limited to goods and services relating to that customer relationship.

This is the law now and this isn't changing. What is changing are the minimum standards you're expected to meet.

**USEFUL LINKS**

**PECR:**
http://www.legislation.gov.uk/uksi/2003/2426/pdfs/uksi_20032426_en.pdf

**ICO PECR Guidance:**
https://ico.org.uk/media/for-organisations/guide-to-pecr-2-3.pdf

**ePrivacy proposal**
https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

**Current draft version**
http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241

**NEW OPT IN RULES**
Under new GDPR rules, opt-in needs to be separated by channel, such as phone, SMS and email. It also needs to be date stamped with reference to the wording used when gathering that opt-in.

Any data gathered before 25th May 2018 where individuals weren't clearly told your data policy, and they didn't consent, will no longer be legal to use. However, if you have a good relationship with your customers, you can re-communicate your privacy policy and gain consent.

Member experts recommend that you avoid using incentives to increase consent and drive opt-ins. Offering a voucher or prize draw implies a condition on individuals to gain the incentive and they should be able to get it without giving consent.

Verifying that an email address is active and the details are correct is referred to as 'double opt-in'. Currently, double opt-in only applies in Germany, but some businesses have adopted it because it increases the quality of genuine captured data for new subscribers and tends to reduce the number of people who unsubscribe.

Single opt-in is generally viewed as a better option for building a marketing list more quickly for a higher quantity of subscribers, but you may have to deal with higher unsubscribe rates, complaints, and blocks (see **Single vs Double Opt-in** below).

| Action | Challenge | Solution |
|---|---|---|
| When you're asking for people's data, be clear and open about exactly what they are opting into | How can you future proof for different uses of data or frequency of communication? Can you still use their data? | If it's in their legitimate interest to receive the new communication, you can use it, but explain this change and include an opt-out |
| If you're sharing data with third parties, list their names for transparency | So much information on an opt-in page can be daunting for prospects who may choose not to give consent | Include the details in your privacy notice with a clearly sign-posted link in the opt-in page |
| Try to keep your opt-in broad enough for its scope to change | Data capture best practice for email marketing is being specific about what the person is signing up to, when they'll receive communication, and why they should sign up | You may need to compromise on your subscriber growth rate to remain GDPR compliant but gain more engaged subscribers |

## Single vs Double Opt-in*

| Issues to Consider | Single Opt-in | Double Opt-In |
|---|---|---|
| **Engagement Rates** | Single opt-in systems tend to show lower open and click percentages than double opt-in. However, they usually have higher number of opens and clicks as they send emails to more people. | Double opt-in systems tend to show higher open and click percentages because people who are subscribed to them actively showed interest in the emails and made effort to receive them. |
| **Complaints from Subscribers** | Emails are more likely to go into junk files, be blocked or be reported as spam. | Emails are less likely to be reported as spam, blocked or put in junk. |
| **Unsubscribe Rates** | There are higher unsubscribe rates for single opt-in processes. | Double opt-in systems tend to have lower unsubscribe rates. |
| **Marketing List Growth** | When sign up processes are quicker and easier, more people are likely to complete their subscription process, and therefore your marketing list is likely to grow quicker. | Marketing lists are likely to grow at a much slower rate with double opt-in systems as people are less likely to complete the signup process. |
| **Evidence of Consent** | Single opt-in provides weak evidence of consent. There's no proof the person who completed the sign up process is the owner of the personal data they provided. | Double opt-in provides stronger evidence of consent. A person wouldn't complete the verification process if they didn't initially sign up to receive email communications. |
| **Protection** | There's less protection against malicious sign ups and spam traps. | Double opt-in provides stronger protection against malicious sign ups and spam traps. |

** Compiled by CommunicatorCorp. Find out more at https://www.communicatorcorp.com/blog/the-GDPR-QA-double-opt-in*

## Member Insight: GDPR FAQs

**Suzanna Chaplin is co-founder of ESBConnect, an email driven customer acquisition platform. A member of The Supper Club, Suzanna is also part of a GDPR hub group working within the DMA to compile a list of questions raised by the industry on different aspects of compliance. This is part of a collaboration between the ICO and DMA to produce practical guidelines for all businesses. Suzanna shares some questions and recommendations:**

**Consent:** A big question is whether consent under PECR and ePrivacy is enough as GDPR requires you to have a legal basis for all of the different uses of personal data. This means having to explain all of the things you're going to do with it before collecting the data, but in a concise way that doesn't put customers off before they've seen the benefits.

The DMA recommends using legitimate interest, explaining why they might be interested based on a prior purchase or enquiry with a clear opt-out and link to relevant sections of your privacy notice.

**Purchased data:** Another key question related to consent is about purchased data, from lead generation or list rental providers, and if Legitimate Interest can be used as the legal basis for marketing. If you want to buy a record for your own use and be the named controller, you will need to get consent at the point the record is collected.

So the lead generator will need to collect data on your behalf and make this clear from the start. If you are not named at point of collection, you can rely on a vertical opt-in but please note the list of vertical cannot be exhaustivse (e.g. list every vertical possible) and needs to be defined e.g. life insurance.

For list rental, the provider is the data controller who sells space in the body of their mailer or newsletter and they will need to justify their support for broadcasting third party content under Legitimate Interest. There is guidance on the new EU website on the GDPR at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/marketing/can-data-received-third-party-be-used-marketing_en

**Suzanna Chaplin, Co-Founder of ESBConnect**

**USEFUL LINKS**

**DMA checklist for marketers:** https://dma.org.uk/article/dma-advice-gdpr-checklist

**DMA guidelines on Legitimate Interest:** https://dma.org.uk/article/dma-insight-the-legal-base-for-legitimate-interests

**DP Network guidance on Legitimate Interest:** https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/

**Historical data:** GDPR is purposefully vague on how long to keep data because of the rapid pace of change in digital communications, but 12 months is the general guideline. This encompasses physical opt-in or engagement (for example, you could have somebody who opted in two years ago but clicked on an email weekly). After 12 months you don't necessarily need to regain consent just prove they are engaged and interacting with your marketing (this may change under e-privacy in 2019) .

One way is to send an updated privacy notice with an opportunity to opt out. If you do choose to keep data beyond 12 months, document the reason as to why with a clear justification (a phone company may justify it on the basis most contracts are for 24 months).

**Incentivising opt-in:** It's common for businesses to use some kind of incentive to encourage people to opt-in, like a prize draw or a free trial. People must have a choice and you cannot force them to enter a competition to opt-in. Under GDPR, they should be able to benefit without giving consent.

**Subject Access Requests:** Businesses have been worried about a PPI style claims industry growing out of SARs, with companies doing it on behalf of individuals. Fortunately, the ICO has specified proof of ID from whoever makes a request which also addresses the risk of giving personal data to the wrong people. If someone raises a SAR for an email address, mobile number or postal address, you can ask for ID and proof of ownership of all three.

Recent cases have also highlighted the risk around SARs from employees. One employee was let go who had been employed for over 20 years and put in a SAR. That's an enormous amount of personal data to compile across all channels. Employees need to have a valid reason, but employers need to take a request seriously.

## Expert Insight: GDPR FAQs

**Peter Galdies is a founder of DQM GRC and DataIQ, a specialist in data governance information solutions to major corporates. DataIQ ran a series of GDPR roundtables for members of The Supper Club and DQM GRC has produced a free GDPR self-assessment. Here he answers some of the key questions raised about GDPR compliance:**

**How long should you keep prospect data?**

Be transparent about how long you will hold data, and why it's reasonable to hold it that long, from the start. The retention period can be longer than 12 months, but it depends on your sales cycle and whether it's a product or service. If it's a two-year sales cycle for a service, for example, you need to demonstrate why that's reasonable with evidence and a narrative to justify it.

Crunch some numbers to find enough who have purchased after a longer sales cycle. You will need to have this to hand for anyone who requests it.

**Do you need to regain consent for prospects before 25th May 2018?**

Legitimate interest may be a better option for communicating with current customers instead of consent. There looks to be a "one-time" opportunity to make this change prior to May 25th. You need to document this decision, the balancing argument for legitimate interest and recognise that this will only be valid for those customers who are currently active. Consent will not be required; instead you will have to offer an opt-out from the processing.

For prospects and lapsed customers, you most likely will have to refresh your consent; but before communicating and asking them to do so ensure that you have a good enough standard or existing consent and that your new consent meet's GDPR's standards. This can be a minefield and we always recommend seeking professional advice if not sure.

**Should you still use incentives to regain consent?**

Incentives can be viewed as marketing and reconsent activity must not be confused with marketing activity. Consent must be specific, unbundled, and granular in communications. Get legal advice but we would generally advise against offering your own products and services as an incentive for consent. In any case the incentive must be available to everyone; they should still receive it even if consent is refused.

**Peter Galdies, Founder of DQM GRC and DataIQ**

GDPR is an opportunity to talk to your customers and prospects as people and build trust and loyalty, so be open about what they will gain by consenting. People tend to self-select, so if they are interested they will and if they are not then they won't – so you will only preach to the converted.

**Is direct mail unaffected by GDPR?**

Direct mail is more flexible for prospecting and is seen in the legislation as a legitimate interest and therefore may not require consent; but you still need to demonstrate that data has been legally gathered and processed, explain how it's going to be used and that you're the data controller.

**Do small businesses need to appoint a DPO, and can it be part of an existing role like marketing or IT?**

There are three criteria specified in the regulation about when you must appoint a DPO. These include being a public body, regularly processing large amounts of special categories of data, and systematically monitoring data subjects on a large scale. The regulation specifies special categories of data this applies to, so it's not payment or contact details but things like sexual or political orientation.

It's unlikely that small businesses will need a DPO, but some small internet businesses might. If you think you should appoint one, then you probably should.

If you don't think you should, you need to write down why not and have that justification to hand (there is good guidance available from the EU working Party 29 which can make this clearer).

A DPO will need to report to the board so it will need to be a senior role and led by someone with the gravitas to drive compliance through the organization.

## Member Insight: Post-GDPR Marketing Plan

**Enrico Brosio is a member of The Supper Club and President of Market One, a global demand generation agency that helps clients in technology, advanced manufacturing, business information and financial services to increase revenue from their marketing activities. Enrico shares his own company action plan for marketing after GDPR.**

**1. Form a Committee:** We've assembled a crack squad to tackle GDPR on all fronts. This includes an executive sponsor from the top and representatives from our global IT function, Data and Technical Services practices and Marketing team - supplemented by an external consultant.

**2. Assess current state:** We've aggregated data from our Eloqua automation platform, NetSuite CRM, and our regional data siloes and run a data audit to find the holes and fill them.

**3. Get ready to receive:** We collect contact data in a number of disparate ways: website form submissions, from outbound calling, through conversations at events or on social media. We'll be leaning on our data services team to structure the marketing database in a way that enables us to report on how and when contacts got in, and if they consented to marketing. Separately, our IT team is looking at how and where we store and handle all data (being ISO27001 certified helps enormously with this effort).

**4. Prepare privacy policies:** We've gathered examples from relevant websites to craft the perfect page.

**5. Forms and confirmations:** We have four forms: contact us, email subscription, content gating and event registrations. We're editing the language used on each so submitters are given a clear and unambiguous option to receive future marketing emails. It's good practice, so we'll apply these changes globally – although we'll probably stop short of requiring a double opt-in via email for markets that don't explicitly require it. Confirmation messages and emails will also be updated to include a 'receipt of consent' and information about link tracking.

**Enrico Brosio, President of Market One**

**6. Build a preference centre:** We've kept it pretty simple for now, giving people the option to receive new articles, event invitations or new product/solution updates. Behind the scenes we'll ensure our emails all map to those categories. Those wishing to unsubscribe will have the option to click the 'snooze' button and stop receiving emails for 6 months.

**7. Proactively drive subscriptions:** We need to give people more opportunity to subscribe to emails. We're also experimenting with some more interruptive formats on the pages that feature our thought leadership content. It makes some people internally a bit uneasy, but we have to have the confidence that if people are spending time with our content, they may welcome the opportunity to subscribe to more of it – as long as there's no hard sell.

**8. Prompt people to opt-in:** We have a program in the works to re-confirm opt-in: four automated emails to be sent over four weeks: one smart, one provocative, one funny, one desperate. Then maybe a 'last chance', followed by a 'very last chance'. Then the difficult decision: to purge or not to purge?

**9. Laser-focused prospecting:** We'll still be using the occasional unsolicited email and outbound calling to prospect for new business within our key target accounts; but we'll do everything we can (using information freely available in the public domain) to ensure each individual we attempt to reach could genuinely benefit from our services. By so doing, we would seek to establish that our communication is in their 'legitimate interest'.

**10. Think beyond email and phone:** We're putting renewed effort into making ourselves findable by optimizing our site for search and launching our first PPC campaign. We'll be increasing our reach and reputation by publishing and promoting articles on LinkedIn and Medium, running webinars and events to build community among our customers, and ramping the co-marketing activity we undertake with partners.

## 8. Children

**GDPR will bring in special protection for children's personal data.**

If your business offers online services to children and relies on consent to collect information about them, you will need a parent or guardian's consent to process their personal data if they are 16 or younger (although this may be lowered to 13 in the UK under GDPR).

If a child is below the age of consent, you will need to get it from a person holding 'parental responsibility' and this will need to be verifiable. When collecting children's data your privacy notice must be written in language that children will understand.

You will need to update your privacy notices to specify age of consent and ensure they are written in a language children will understand. You will also need to update your data collection to ask for their parent's credit card details to verify their consent.

## 9. Data Breaches

**The GDPR places a duty on organisations to report certain types of data breach to the ICO, and in some cases, to individuals.**

You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

If it's a high risk, you will also have to notify those concerned directly. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

If you breach GDPR legislation, individuals can claim damages without the need to show any evidence of harm to support their claim. A breach means any breach of the law, not just a breach of security or a hack. The larger fines are reserved for things like a breach of consent rather than security (where the fine is half of this).

If you breach GDPR law, the maximum you can be fined is €20m or 4% of your global turnover, whichever is larger. A breach could be that you have been negligent in protecting people's rights; or you don't have the right consents to contact them in a certain way, with a certain message at a certain frequency.

**WORKING WITH THE ICO**

In any documentation showing the precautions you have taken, the ICO will want to know:

- Where the data came from
- When and how it was gathered
- What was the basis for consent
- How it's been used
- What your policy on data retention is

If you're selected for audit, the ICO will ask you to participate voluntarily but it will be compulsory if you don't respond.

| Action | Challenge | Solution |
|---|---|---|
| Put procedures in place to effectively detect, report and investigate a personal data breach | You may not find out about a breach until someone makes a complaint. | With email/phone/text communication, check that you have explicit consent and you're only communicating what they have specifically indicated they want to be contacted about. If in doubt, don't contact. Ensure your data systems have adequate security in place |
| Assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred | Historic data - where you have no record of how, when or why the data was captured - is difficult to assess accurately | If you can't prove consent was given, you will need to delete it |
| Nominate someone to manage this process and make prompt notifications to all concerned | Who will monitor and report data breaches and how will they know if they have reported it in time? | Hire a specialist initially to work with your team to put in place the processes and procedures to detect, investigate and report a breach and train staff handling data to monitor and report |

## Member Insight: IT security checklist

**Steve Clarke is a member of The Supper Club and Co-founder of Freeman Clarke, which provides part-time 'fractional' IT Directors, CIOs, and CTOs. Steve shares five tips to help business owners manage their data security**

**Steve Clarke, Co-founder of Freeman Clarke**

• **Privileges:** Access to systems should be on a least-privilege policy. For example, when a person is given access to a system, the default should ensure that person has no rights to anything.

Then privileges should be granted according to what that person needs to do in the system, building up to only include the data and processes they require. If your systems don't follow a least-privilege system, then you are significantly exposed to cyberattack, to fraud and to errors.

• **Prevention:** All computers should use up to date operating systems with up to date anti-virus and anti-malware systems; but these systems only work well when they know what they're up against.

Newer protection systems coming on to the market look for programmes acting suspiciously and will automatically shut the programme down before it has had time to cause mayhem. These systems provide protection against new attacks (called 'Zero Day') because they spot the bad behaviour of an application rather than recognise the malware itself.

• **Protection:** To protect your data, it should be encrypted by default and only accessible to those with the approved rights to look at it. Where you have customer data, particularly user accounts and passwords, ask your IT team whether the data is 'hashed and salted' which will make it very secure and difficult to break even if your systems are breached. It is unforgiveable nowadays to be holding customer data unencrypted (known as 'clear or plain text').

• **People:** Criminals have become highly adept at social engineering. For instance, emailing your financial controller posing as you, the CEO, telling them to send money to a supplier and providing bank account details are not unusual.

Many people fall for this and a lot of money can be lost very quickly. Create a 'secure culture' where taking this stuff seriously is encouraged. Ensure you and the Board demonstrate good practice. For example, if you write your passwords on post-its then you should fully expect your staff to do the same.

• **Principal:** Who's in charge if you're attacked by ransomware and decisions need to be taken on the spot? GDPR makes specific requirements about notifying the ICO if you suffer a security breach. Decide who is responsible for making this happen; as failure to do so will result in a fine.

## 10. Data Privacy By Design

**GDPR requires organisations to show they have made their data processing compliant with the concept of 'privacy by design' (compliance from the start). To achieve this, GDPR specifically refers to encryption and pseudoanonymization to avoid security risks.**

You must also use Data Privacy Impact Assessments (DPIAs) for processing 'high risk' activities, which includes monitoring. This is continual and ongoing; so if you haven't recruited a DPO you still need someone to monitor and manage this.

You will need to ensure that your systems are penetration tested regularly and conduct ongoing DPIAs. Review your security measures and policies to make sure they are GDPR-compliant – or get them in place.

If you use encryption, make sure it's robust enough to protect you from a breach and consequent penalties.

People are often the weakest link in security, so train your employees to understand what constitutes a personal data breach, any processes to highlight any red flags, and why it's important to report a serious breach within 72 hours.

**Conduct** a full audit of your systems to identify and address any weaknesses and conduct ongoing DPIAs

**Consider** bringing in a data security and compliance specialist to conduct the audit and train your team

## 11. Data Protection Officers

**The primary role of a DPO is to ensure everyone in an organisation is fully compliant with GDPR. The level of knowledge required will depend on the technical nature of your business as well as the number of controllers and processors of data.**

The DPO will need to keep the board and employees informed about data protection requirements, monitor compliance with GDPR, manage staff training, conduct audits and reviews, provide advice on any impact assessments, and liaise with the supervisory authority. Employers may need to recruit supporting staff or provide a training budget to enable the DPO to carry out these tasks and maintain their expert knowledge.

Currently, you only have to appoint a DPO if you are a public body, regularly process large amounts of data, or systematically monitor data subjects on a large scale. This applies to special categories of data under GDPR, such as sexual or political orientation and not payment or contact details.

“It’s unlikely that small businesses will need a DPO, but some small internet businesses might,” says Peter Galdies, Founder of DataIQ. “If you think you should appoint one, then you probably should. If you don’t think you should, you need to write down why not and have that justification to hand."

“It can be part of an existing role, but nothing can impede or conflict with their tasks and responsibilities as DPO", adds Galdies. “A DPO must report to the board so it will need to be a senior role and led by someone with the gravitas to drive compliance through the organization.”

## 12. International

**If you have offices around the world, there are restrictions on what data can be transferred between certain countries.**

Under the current Data Protection Act, personal data ‘shall not be transferred to a country or territory outside the European Economic Area (EEA)’, which includes all of the EU member states plus Iceland, Liechtenstein, and Norway.

You will need to map out where your organisation makes its most significant decisions about its processing activities to help determine your main establishment and your lead supervisory authority.

Data can be stored outside the EU, in the US for example, but sufficient safeguards must be in place when transferring data out of the EU. While the US doesn’t meet the GDPR’s requirements for the transfer of data out of the EU, Privacy Shield allows US companies, or EU companies working with US companies, to meet them.

Some experts recommend a General Data Processing Agreement (GDPA) between organisations inside and outside the EU.

“This is a legal document signed and adopted by all companies within a group, which sets out how they all agree to secure and protect personal data they share,” explains entrepreneur and adviser Peter Borner.

“If you cannot get a GDPA then you have to rely on standard clauses (as defined in the GDPR). Simply relying on the US Privacy Shield is not sufficient. All transfers to third party countries will have to be correctly and fully documented in your Article 30 records.”

| Action | Challenge | Solution |
|---|---|---|
| Undertake an audit, create robust processes, train staff, test systems, and track risk in board reporting | Who will be responsible for this and is all of the knowledge about systems and processes (historic and current) needed to complete this task held in-house? | Create a working group of individuals across teams who can get a thorough understanding, identify gaps, and agree actions to address them |
| Decide if you are going to recruit a specialist to manage this or someone with the right aptitude and skill set in your business who can be trained | Though most small businesses aren’t required to recruit a DPO, they can be penalised in the same way as larger businesses | Is there a way to justify the cost of recruiting a specialist full or part time to help differentiate and protect your business? |
| Review any overseas partners and processes to check where data is stored and where it is transferred | Several Email Service Providers and CRM servers are located outside the EEA (in the USA especially) | Identify where your data server is located and check how your data is protected |

## Member Insight: Choosing a specialist

**Joanne Smith is a member of The Supper Club and founder of TCC Group, a consultancy which helps businesses to effectively navigate regulatory change. TCC has a free GDPR preparedness assessment online at https://www.tcc.group/2017/09/12/gdpr-preparedness-assessment/. With an explosion in the number of consultants offering GDPR compliance services, Joanne shares five tips on choosing the right consultancy and getting the most value from the partnership.**

Joanne Smith, Founder of TCC Group

1. **Genuine experience:** Due to the relative newness of GDPR you are unlikely to find much differentiation in consultants' experience in this specific field. One way to differentiate is to find a consultancy that are not only GDPR specialists, but also have a track-record in helping businesses comply with other types of regulatory change. These experts should be able to offer tailored support using tried and tested frameworks, methodologies, and tools for successful compliance rather than off-the-shelf advice. This may be a more expensive option, but it will stand up to ICO scrutiny.

2. **Broad understanding:** You might not need to outsource everything and only need advice and guidance. The only way to decide this is to understand the full journey for getting GDPR compliant. A good consultancy will explain what this looks like and help you to find your internal gaps in knowledge, skills, and resource that they can fill. This will help to prevent you paying for services you don't need.

3. **Practical not theoretical:** Whether you're using a consultancy for advice or implementation, guidance must be practical to have an impact. Making sense of 'what' GDPR is and its requirements is all very well, but the real value is in 'how' you ensure and evidence compliance. Can your consultant provide you with tactics, tools and actions that should be implemented, not just a regurgitation of the rules and principles?

4. **Commercially aware:** GDPR may seem like an exercise in box-ticking but there is commercial value to be found if you're willing to take advantage of it. A good consultant will help you to comply with the spirit of the rules as well as simply adhering to them. They can help you to build a closer and more trusted relationship with your clients, improve customer retention and increase confidence in new prospects. GDPR is an opportunity to reconnect with old clients and reassure new ones; but do it before the GDPR noise as we get closer to the deadline.

5. **Your responsibility:** Regardless of which aspects of GDPR compliance you outsource, you and your board are ultimately responsible. GDPR has board level accountability, so someone at the top of your organisation needs to not only be familiar with the requirements but also be aware of what the team and outsourced supplier are doing to ensure compliance. If you neglect this responsibility, you could spend more than you need to and leave your business open to potential risk.

## Conclusion

While much of rhetoric around GDPR compliance is about threat and burden, it should be seen as a positive opportunity for businesses to change their mindset on customer and employee data. Instead of hoarding data and adding to the barrage of unwanted emails, you can communicate with the right people at the right time in the right way for the best outcome.

The investment of time and resource in defining processes and updating systems will improve efficiency. Training everyone in your business to understand the risks and consequences of a breach will help to make people more aware and responsive to risks.

Smaller businesses may find it easier to monitor and manage risk with fewer people to train and manage; but embedding a culture of compliance in any size of team will require investment. This will mean working with specialists in most cases, even if it's just to lay a solid foundation of systems, processes, and training.

With so many consultants emerging over the last year offering GDPR compliance audits and training, business owners will need to choose carefully.

This is a board level issue that requires regular monitoring and reporting in the risk register. GDPR will require leadership, and not just at board level. Businesses will need people to manage and monitor risk, whether it's a specialist DPO or someone trained within their existing team to become one.

Those who have prepared early are already looking beyond compliance to how they can differentiate and win more business.

> "This law is not about fines. It's about putting the consumer and citizen first. We can't lose sight of that … It's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm."

**Elizabeth Denham, UK Information Commissioner**

## GDPR Compliance Checklist

| | | |
|---|---|---|
| Awareness | Are senior decision makers and key people in your organisation aware of changes to data protection under and the consequences of any breaches? | |
| Stored information | Have you documented what personal data you hold, where it came from and who you share it with? | |
| Communicating privacy | Have you reviewed your current privacy notices and put a plan in place for making any necessary changes? | |
| Individuals' rights | Do you have a process for deleting personal data or providing data in a commonly used format for those who request it? | |
| Subject access requests | Do you have a process to provide a machine-readable copy of any personal data within 30 days of a request? | |
| Processing personal data | Have you defined and documented your legal basis for processing different types of personal data? | |
| Consent | Have you reviewed how you seek, obtain and record consent and do you need to make any changes? | |
| Children | Do you have a system in place to verify individuals' ages and gather parental or guardian consent for data processing? | |
| Data Breaches | Do you have a process in place to detect, report and investigate a personal data breach? | |
| Data Privacy by Design | Have you identified any high-risk areas of data processing that will require Data Privacy Impact Assessments? | |
| Data Protection Officers | Have you designated a DPO or recruited someone to take responsibility for data protection compliance? | |
| International | Have you determined which data protection supervisory authority you come under for the movement of data? | |

# Could You Benefit From Membership of The Supper Club?

**If you would like to join The Supper Club and its extraordinary community of inspiring entrepreneurs, here are our criteria to be considered for membership:**

• Only the founder & CEO can be a member, not their business but senior managers can attend our workshop and speaker led events

• Your business must have at least 20% sustained growth with a minimum turnover of £1million or have raised on a valuation of £5million and have a minimum of 10 staff. For agency style businesses the minimum turnover is £3million with 20 staff

• Membership excludes consultants, professional and financial services, one-man bands, life coaches, mentors and anyone only interested in selling to our members

• The Supper Club is industry agnostic, B2B and B2C, so members can connect and learn from peers across a range of businesses and sectors to retain a good balance, we occasionally restrict membership from certain sectors

THE SUPPER CLUB

"Every time I have gone to an event, I have come away with such an amazing positive energy, a list of things to improve within the business and networking contacts. I think it's the best investment in time you can make."

**Cecile Reinaud, Founder, Seraphine**

**THE RULES**

• We have a Give and Get ethos to maintain a community where members help and learn from peers

• The Chatham House Rule applies to all of our roundtable events so members can be open and honest

• Overt selling is not allowed, although it is not uncommon for our members to discover business opportunities with fellow members

**THE MEMBERSHIP**

We have several membership options for founders & CEOs, and programmes for your senior managers. We consider all applications on their own merits and we meet all potential members face to face toensure a good fit and a commitment to the Club's values, culture and ethos

**If you would like to explore membership of The Supper Club and the ways it could help you and your business, then get in touch by calling our team on 020 3697 0810 or by emailing getintouch@thesupperclub.com**


thesupperclub.com