Action to take first

The deadline for the not-so-new European Union data protection law called the General Data Protection Law (GDPR) is on Friday, 25 May 2018. The two-year grace period ends on Thursday and on Friday everyone to whom it applies must comply. (Are you at the beginning of your journey to protect data? Are you chasing a deadline to be ready (or compliant) by a certain date?) It is unlikely that an

Programme Index

Hover over the menu below and click on the breadcrumb above to navigate your way through the programme.

authority or a regulator is going to fine you straight after the deadline but if you fail to protect personal data, you might lose a few customers, suffer reputational damage, or have to pay damages to data subjects.

- Must your organisation comply?
- What should your organisation prioritise?
- What should you do first?

Some organisations have been working towards compliance for some time but are not there yet. Others have left it to the last minute and are now trying to start their compliance efforts. Others don't even know it exists or where to start. If you fall into one of these categories, don't stress – we can help.

We can help you to determine whether you must comply with the GDPR. If you must comply, in this module we will give you a list of the things (about 15) we believe you should do first, ranked in order of importance. Many people (like the ICO) have published lists of what they believe you should do first. We've read those lists and based on our experience we have created our own list. Of course, the list will be different for each organisation and it is important for you to work out what the list is for your specific organisation. This is not necessarily a list of quick wins. This is a list of things to do first or as soon as possible.

Introduction

Who is responsible?

The officer – either the information officer or the data protection officer.

Is it too late?

Yes, and no. If you need to comply with the GDPR, you're late but don't worry you're not alone. Data protection compliance is a journey rather than an event or destination. It is very hard for anyone to say at any point in time that they are fully compliant. Everyone is continually working towards compliance and responding to changes in their activities and the world. It takes years to get data protection right and it is not possible to get it all done overnight.

What does it cost?

Lots. According to the FT "Companies in the UK's FTSE 100 are estimated to have had to spend an average of £15m each" and "Global 500 will spend a combined $7.8bn on compliance, an average of almost $16m each". You probably can't spend anywhere close to that.

How do we prioritise?

We use a number of factors which we have covered in a previous module of the programme. If you are starting now it is important to follow a risk-based approach and start doing things with the risks of non-compliance in mind.

Learn from other jurisdictions

You should start off by appointing someone within your organisation to conduct research and to help fast track the data protection programme. Try find other organisation's which are similar to yours, in mature jurisdictions like Germany or the UK (try sticking to the EU). Go look on these organisation's websites at how they've done their privacy policies.

Brief your governing body

You should also make sure that the key people and decision makers within your organisation appreciate the impact the GDPR will have. You should do this as soon as possible. See our Governance module.

Appoint an EU representative

If the organisation is processing personal information of EU citizens outside the EU, the GDPR requires a representative in the EU to act as a contact point. This representative can either be a legal entity or a natural person. It is up to you who you choose. We can help point you in the right direction if you need guidance.

Appoint a data protection officer

If you are processing a lot of personal data or special personal data such as medical records, then you will need a data protection officer (DPO). A DPO can be an existing staff member. You need to decide how many officers are needed in your organisation and how will they be structured. Once you have decided who is the best person for the position and you must appoint them and their deputies using a formal letter (ask us for the draft proposed letter). You will then need to update your PAIA manual to include the name and contact details of your new officer. See our Governance Module for more information.

Create an EU one-stop shop

Create a one-stop shop in the EU by identifying the lead supervisory authority that would suit your organisation best. As a starting point, check whether there's a specific concentration of customers in a particular jurisdiction in the EU. That jurisdiction might work best for you. See our Regulatory Bodies module in the Michalsons Data Protection Compliance Programme.

Plan your incident response or breach management

Awareness training is very important when it comes to incident response, as it can help mitigate any problems. Planning your incident response should be high up on your priority list, as you want to deal with any breaches as effectively as possible. To increase your employees' awareness about incident response, they can watch the Incident response readiness module in the Michalsons Information Security Compliance Programme. After you have watched the module, you can then update or supplement your organisation's existing response policies and procedures.

Get cyber insurance

Has someone in your organisation gone through the Cyber or Data Protection Insurance module? Make sure your organisation has an agreement with a reputable insurance company to protect you from financial loss if a cyber risk materialises. For example, a cyber risk could be a data breach, hack or any other unlawful access to data containing personal information. You can even check with your current insurer to see if they can change/update your existing policy to include cyber insurance.

Have a complaints procedure

From the 25th of May data subjects will have a lot more rights and will want to exercise them. You should establish actions to take when someone lays a complaint against your organisation. Remember to make sure your complaints procedure is user-friendly and easy to find so unhappy customers will go to your organisation first and not to the regulator. You must train your employees on how to handle data protection complaints effectively so the unhappy customer will be less likely to go to the regulator. You can create scripts for your help centre on data protection, so they can address the complaint adequately and efficiently. See our Quick Wins module of the programme for more information.

Update customer-facing documentation

You should update your privacy policy and terms of service so that they are GDPR compliant. You have worked hard to gain the trust of your customers. When they go onto your website make sure it is easy for them to see how you are protecting their personal data by updating all your existing policies. Then

you can inform your customers of the changes made and reasoning behind those changes (prioritise your customers and inform your most important clients first). You can also prepare a response talking generally about the GDPR and your organisation's compliance plan.

Manage the relationship with customers who are controllers

With the GDPR deadline commencing, many organisations are currently fielding requests from their customers as responsible parties to complete questionnaires and sign data processing agreements related to the GDPR. You should develop relevant knowledge and skills within the organisation so your employees can properly complete the customer questionnaires. When you negotiate new customer agreements they should all contain GDPR wording. You should also remember to update existing customer agreements by adding GDPR wording.

Agree to data processing agreements

You need to incorporate the relevant clauses into the organisation's standard terms and you should try not to conclude any separate data processing agreements. You need your customer-facing documents to be able to explain why you don't need to sign separate agreements.

Minimise access to sensitive data

Minimising access to data is a key data protection principle.Think to yourself, where in my organisation do we have the most personal data stored and would cause the most harm if a criminal got hold of it? Make sure only select people within your organisation can access sensitive data such as identity numbers, health records, race information, biometric data etc. When you can, try encrypt or obfuscate the sensitive data. You should also limit how long sensitive data is stored for and delete any sensitive data, when the data subject is no longer a customer of yours.

Decide to follow privacy by design strategy (PbD)

When you start a new project, make sure that it is started with privacy in mind. Have a plan on how new projects should be started. You can use privacy impact assessments to begin with and then communicate the privacy plan to your customers. The privacy by design approach means any problems your organisation might have will be identified from the outset. This approach will also help your organisation meet the legal obligations expected of you under the GDPR. See our Privacy by Design module of the programme.

Enable the right to be forgotten (subject access and deletion requests)

You and your organisation must formalise a plan of action to take when a data subject asks for access to their personal information. You should implement a procedure for deleting a data subject's data off your databases when they ask you to. However, if you can show legitimate grounds for processing the data or when you process personal data in order to establish, exercise or defend legal claims, then you may still retain certain personal data. On your website, you can add a page where customers can ask for access to their data and the procedure on how to get their data deleted. You need to be able to service these requests so your customers don't complain to the regulator about you. See our module on Data subject participation.

Enable data portability

Data portability is a key principle in the GDPR but it only applies to information being processed with the data subject's consent or pursuant to a contract. So data portability is not always relevant to everyone. It is intended to give data subjects more control over their personal data. You will need to establish a plan of action when a data subject requests to move their data and it should be done in a user-friendly manner. See our Data Portability module.

Manage your relationship with your service providers as processors

It is important that you take steps to make sure that your processors are processing personal information lawfully on your behalf. You will need to identify and record all your existing processors from your list of current contracts. Then we suggest, you rank their level of risk based on the sensitivity and volume of the information that they process on your behalf. Ask them how they go about protecting the personal information. You will then need to negotiate changes to the existing or new contracts with them, with better or added GDPR clauses. Remember to always reduce or eliminate the amount, or kinds of personal data that you give them.

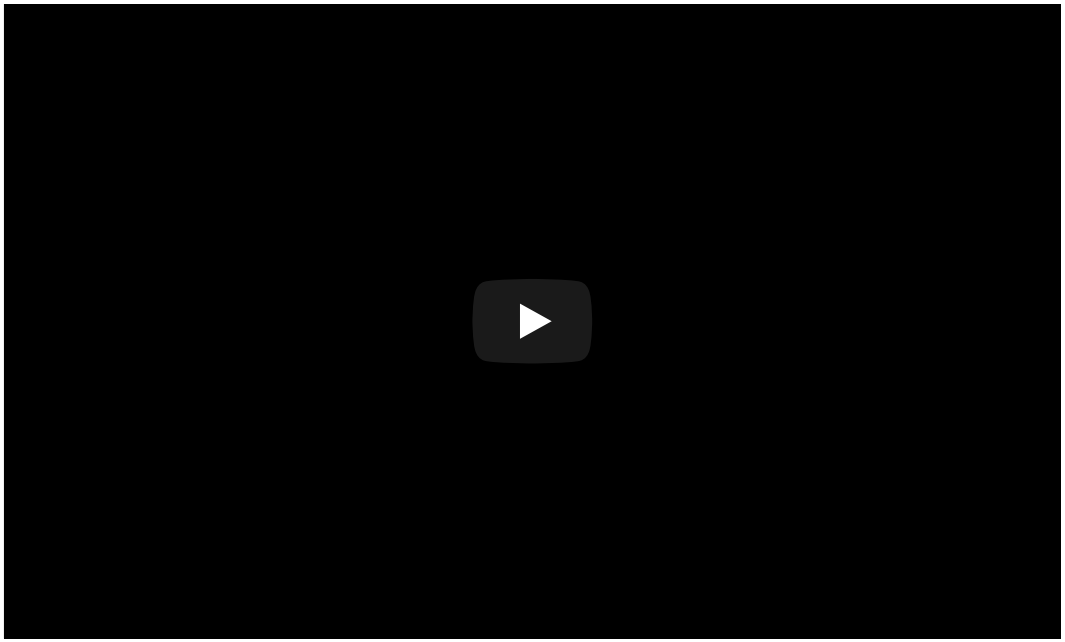
Useful resources

- Article on the Financial Times about Wake-up call to business with one month to be GDPR-compliant
- ICO guide on preparing for the GDPR 12 Steps to Take Now
- Top ten tips to prepare for the GDPR
- 10 Things You Need To Know To Prepare For GDPR
- The Hubspot GDPR Last-minute kit

Actions

1. Get certainty on whether or not you have to comply.
2. Work out what you need to do in the next two days.
3. Work out your list of top ten things to do in the next 30 days.

Video for this module



Next

MEMBERS AREA

- Programmes
- Laws
- Tools
- Events
- Recordings
- Communities
- Support

INSIGHTS

- Michalsons recognised as leading IT Lawyers
- ICT Weekly Update
- Film and Publications Bill – Internet Censorship?
- Differences between King III and King IV
- Reseller Agreement – Agent or Distributor?

VISIT PUBLIC AREA

Remember that you are currently in the members area. You can always visit the public area of the Michalsons website.

NEED HELP?

If you need support using the members area, please email our Support Desk or contact 0860 111 245.

RELATED

1. A Compliance Action Plan is Essential
2. Information Rights Complaint | Action to Take
3. Information Security Action Items: A set of checklists
4. What is a Data Protection Officer?