DMA Nonprofit Federation

Data & the EU General Data Protection Regulation

12 Tips to Prepare for GDPR Compliance

The General Data Protection Regulation (GDPR) is in effect for organizations active in the EU on May 25, 2018 and replaces the European Data Protection Directive in all EU member states. The GDPR does not exempt nonprofit organizations, which collect a great deal of personal information and must comply with the GDPR. The fines are very steep: 4% of annual turnover or 20 million euros, whichever higher. Take time now to review the key steps needed for compliance. Please note that this update does not replace legal advice — please review the GDPR and its impact with your own legal counsel. If you have questions or require assistance, contact DMANF's Senny Boone at SBoone@thedma.org. The key points below were developed in conjunction with the Email Experience Council.

1. Awareness

You should inform decision-makers and key people within your organization about the EU General Data Protection Regulation (GDPR). Assess the impact it is likely to have and identify areas that may create compliance problems under the GDPR. It would be useful to start by looking at your organization's risk committee, if you have one.

Compliance will be difficult if you leave preparations until the last minute. Prepare, prepare and prepare!

2. Information you hold

You should document what personal data you are in possession of, where it came from and with whom you share it. You may need to organize a full information audit, across the entire organization, or within a particular business area.

- The GDPR updates rights for a networked world. For example, if you have inaccurate personal data and have shared it with another organization, you must tell the other organization about the inaccuracy so it may correct its own records. You would not be able to do this unless you know what personal data you hold, where it came from and with whom you share it. You should document it and maintain it. In doing so, you comply with the GDPR's accountability principle, which requires organizations to demonstrate how they comply with the data protection principles.

3. Communicating privacy information

Review your current privacy notices, statements and policies and make any necessary changes in time for the GDPR implementation.

- Your privacy notice should disclose your information collection, use, sharing and protection practices. Under the GDPR, there are some additional requirements. For example, you will need to explain your legal basis for processing the data; your data

retention periods and that individuals have a right to contact the Information Commissioner's Office (ICO), or whichever Data Protection Authority (DPA) you fall under, if they believe their data privacy complaint was not resolved directly by your organization. Note that the GDPR requires your privacy notice be concise, easy to read and understand. (This is a current DMA Guideline requirement.)

4. Individual rights under GDPR

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The main rights for individuals under the GDPR will be to:

- access data,
- have inaccuracies corrected,
- have information erased,
- prevent direct marketing,
- prevent automated decision-making and profiling, and
- have ability to data portability.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to develop a plan if someone asks to have their personal data deleted, for example. Would your systems be able to easily locate and delete the data? Who will make the decisions about deletion? Who needs to be involved? The policies and procedures around this need to be fine-tuned.

The right to data portability is new. This is an enhanced form of consumer access where you have to provide the data electronically and in a commonly used format. Many organizations will already provide the data in this way, but if you use paper print-outs or an unusual electronic format, now is a good time to revise your procedures and make any necessary changes.

5. Consumer access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

The rules for dealing with subject access requests will change under the GDPR. In most cases, you will not be able to charge for complying with a request and normally you will have just a month to comply, rather than the current 40 days. There will be different grounds for refusing to comply with subject access requests – manifestly unfounded or excessive requests may be charged for or refused. If you want to refuse a request, you must have policies and procedures in place to demonstrate why the request meets these criteria for refusal.

You must also provide some additional information to people making requests, such as your data retention periods and the right to have inaccurate data corrected. If your organization handles a large number of access requests, the impact of the changes could be considerable so the logistical implications of dealing with requests more quickly and providing additional information will need careful consideration. It may ultimately save your organization a great deal of administrative cost if you develop systems that allow people to access their information easily online. Organizations should consider conducting a cost/benefit analysis of providing online access.

6. Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

Many organizations will not have thought about their legal basis for processing personal data. Under the current law, this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your legal basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your legal basis for processing.

You will also have to explain your legal basis for processing personal data in your privacy notice and when you answer a subject access request. The legal basis in the GDPR is broadly the same as those in the DPA so it should be possible to look at the various types of data processing you carry out and to identify your legal basis for doing so. Again, you should document this in order to help you comply with the GDPR's 'accountability' requirements.

6. Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

Like the DPA, the GDPR has references to both 'consent' and 'explicit consent'. The difference between the two is not clear given that both forms of consent have to be freely given, specific, informed and unambiguous. Consent also has to be a positive indication of agreement to personal data being processed — it cannot be inferred from silence, pre-ticked boxes or inactivity. If you rely on individuals' consent to process their data, make sure it will meet the standards required by the GDPR. If not, alter your consent mechanisms. Note that consent has to be verifiable and that individuals generally have stronger rights where you rely on consent to process their data. Data consent must be specific — consent for one specific occasion cannot be implied to future instances. Also, you should provide for consent revocation — it should be as easy to revoke consent as it is to provide consent.

The GDPR is clear that controllers must be able to demonstrate that consent was given. You should therefore review the systems you have for recording consent to ensure you have an effective audit trail.

6. Children's data

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial Internet services such as social networking. In short, if your organization collects information about children — in the UK this will probably be defined as anyone under the age of 13 — then you will need a parent or guardian's consent in order to process their personal data lawfully. This could have significant implications if your organization aims services at children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

7. Data breaches

Make certain you have the right procedures in place to detect, report and investigate a personal data breach.

Some organizations are already required to notify the Information Commissioner's Office (ICO) and potentially other bodies when they suffer a personal data breach. However, the GDPR will usher in a breach notification duty across the board. This will be new to many organizations. Not all breaches will have to be notified to the ICO — only ones where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach.

You should start now to make sure you have the right procedures in place to detect, report and investigate a personal data breach. This could involve assessing the types of data you hold and documenting which ones would fall within the notification requirement if there was a breach. In some cases, you will have to notify the individuals whose data has been subject to the breach directly, for example where the breach might leave them open to financial loss. Larger organizations will need to develop policies and procedures for managing data breaches – whether at a central or local level. Note that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

8. Data protection by design and data protection impact assessments

You should familiarize yourself now with Privacy Impact Assessments (PIAs) and work out how to implement them in your organization (if you need to). There

is plenty of guidance on this and it shows how PIAs can link to other organizational processes such as risk management and project management. You should start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

It has always been good practice to adopt a privacy by design approach and to carry out a privacy impact assessment as part of this. A privacy by design and data minimization approach has always been an implicit requirement of the data protection principles. However, the GDPR will make this an express legal requirement.

Note that you do not always have to carry out a PIA — a PIA is required in high-risk situations, for example where a new technology is being deployed or where a profiling operation is likely to significantly affect individuals. Note that where a PIA (or DPIA as the GDPR terms it) indicates high risk data processing, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

9. Data protection officers

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organization's structure and governance arrangements.

The GDPR will require some organizations to designate a Data Protection Officer (DPO), for example, public authorities or ones whose activities involve the regular and systematic monitoring of data subjects on a large scale. The important thing is to ensure that someone in your organization, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to do so effectively. Therefore, you should consider now whether you will be required to designate a DPO and, if so, to assess whether your current approach to data protection compliance will meet the GDPR's requirements.

10. International considerations

If your organization operates internationally, you should determine which data protection supervisory authority you come under.

The GDPR contains quite complex arrangements for working out which data protection supervisory authority takes the lead when investigating a complaint with an international aspect, for example where a data processing operation affects people in a number of Member States. Put simply, the lead authority is determined according to where your organization has its main administration or where decisions about data processing are made. In a traditional headquarters (branches model), this is easy to determine. It is more difficult for complex, multi-site companies where decisions about different processing activities are taken in different places. In case of uncertainty over which supervisory authority is the lead for your organization, it would be helpful for you to map out where your organization makes its most significant decisions about data processing. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

Thank you

A special thanks to DMA's Email Experience Council (eec) and James Koons; Chief Privacy Officer, dotmailer; member of the eec Advocacy Subcommittee and lead author of this tip sheet. The eec is the email marketing arm of the Data & Marketing Association. ■

View full document @
https://gdpr-info.eu/