ESPC
Email Sender & Provider Coalition

PREPARING FOR THE GDPR?

Preparing for the General Data Protection Regulation

1 September 2016

The Email Sender & Provider Coalition

ABOUT THE GDPR

- First proposed in January 2012
- Formally approved in April 2016
- Comes in to force on 25 May 2018
- Will supersede national laws
- Is meant to unify data protection and ease flow of personal data
- All organizations processing PII of EU residents must comply
- Significant penalties

ABOUT THE GDPR

The final text of the GDPR can be found here:

http://jko.io/thegdpr

KEYS TO PREPARING FOR THE GDPR

- Start planning your approach to GDPR compliance NOW
- Secure buy-in from key people (senior execs and board members)
- Evaluate the differences between the current law and the GDPR – concentrate where you have gaps
- The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate **accountability**
- Certain parts of the GDPR have more of an operational impact on some organizations than on others

12 THINGS TO TAKE A LOOK AT NOW

- Awareness
- Information You Hold
- Communicating Privacy Information
- Individuals' Rights
- Subject Access Requests
- Legal Basis
- Consent
- Children
- Data Breaches
- Data Protection by Design & Data Protection Impact Assessments
- Data Protection Officers
- International

AWARENESS

- Key Individuals (C-suite and board memebers)
- Appreciation of the impact
- Do you have a risk register / risk committee?
- Know what resource commitments may be required
- Use this two year lead period to raise awareness

INFORMATION YOU HOLD

Conduct a full data audit across the entire organization:

- Document what data you have (and where you got it from)
- Document who you are sharing data with

Knowing what data you have, where it came from and who you are sharing it with will help you comply with the GDPR's accountability principle.

COMMUNICATING PRIVACY INFORMATION

- Review your current privacy policy / privacy statement
- Privacy notices server to let individuals know who you are and how you intend to use their data

You need to explain:

- Your legal basis for processing data
- Retention periods
- That individuals can complain to a DPA if there is a problem

This all has to be done in concise, easy to understand and clear language!

INDIVIDUALS' RIGHTS

Rights for Individuals:

- Subject access
- To have inaccuracies corrected
- To have information erased
- To prevent direct marketing
- To prevent automated decision-making and profiling
- Data portability

SUBJECT ACCESS REQUESTS

- The rules for these requests will change under the GDPR
- No charge in most cases
- You would only have 30 days to comply
- You also need to have policies/procedures for refusing requests
- Retention policies and correction policies have to be given

Consider conducting a cost/benefit analysis of providing online access.

LEGAL BASIS FOR PROCESSING PERSONAL DATA

- Review & document your legal basis for processing
- Legal basis must be explained in your privacy notice
- Legal basis must be explained in access requests

Document this as it helps to comply with the GDPR's accountability requirements.

CONSENT

- GDPR references both consent and explicit consent with no clear difference
- Make sure your consents meet the standards required
- Consent has to be verifiable and data subjects generally have stronger rights when consent is relied on for processing
- CONTROLLERS MUST BE ABLE TO DEMONSTRATE THAT CONSENT HAS BEEN GIVEN! – Make sure you have an audit trail
- Think CASL

CHILDREN'S DATA

- Special protection for children's personal data
- Age verification mechanism
- Parental / guardian consent

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.

DATA BREACHES

- NEW: breach notification requirement across the board
- Procedures for response and reporting

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.

DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

- Familiarize with Privacy Impact Assessments (PIA) and how to implement them in your organization
- Assess when a PIA will be necessary
- Adopt privacy by design

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.

DATA PROTECTION OFFICERS (DPO)

- Only certain organizations will be required to appoint a DPO
- If you don't require a DPO – appoint someone to be the lead

A DPO must be "all about data protection" and careful consideration has to be taken when it comes to their place within an organization. The GDPR expressly prevents dismissal or penalty of the data protection officer for performance of their tasks.

INTERNATIONAL CONSIDERATIONS

- Which DPA do you fall under?
- Complex arrangements for working out which data protection supervisory authority takes the lead

Put simply, the lead authority is determined according to where your organization has its main administration or where decisions about data processing are made.

QUESTIONS?

James Koons

Email Sender & Provider Coalition

james.koons@dotmailer.com

Twitter: @Email_Privacy

ESPC
Email Sender & Provider Coalition