



# GDPR Readiness Assessment for Customers

**8 STEPS TO BE READY**

**General  
Data  
Protection  
Regulation**

**COMPLIANCE  
DEADLINE**



## **1** COLLECTION

- At the time when you collect information about individuals, are they made aware of the uses for that information? (website, forms)
- Are people made aware of disclosures of their data to third parties? (processors)
- Have you obtained consent for any secondary uses of their personal data, which might not be obvious to them (terms)?
- Can you describe data collection practices as transparent? (terms)

## **3** SECURITY

- Is there a list of security provisions in place for each data set? (access)
- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data you keep?
- Are computers and databases password-protected, and encrypted if appropriate?
- Are computers, servers, and files securely locked away from unauthorised people?

## **2** PURPOSE

- Are you clear about the purpose (or purposes) for which you collect and keep personal information? (newsletters, promotions, events, etc)
- Are the individuals in your database also clear about this purpose?
- Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each? (internal roles and responsibilities)

## **4** RELEVANT & MINIMAL

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard? (privacy policy)

## 5 ACCURATE AND UP-TO-DATE

- Do we check our data for accuracy? (process)
- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated? (purpose)
- Do we take steps to ensure our databases are kept up-to-date?

## 7 THE RIGHT OF ACCESS

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures ensure compliance with GDPR requirements?

## 6 RETENTION

- Is there a clear statement on how long items of information are to be retained?
- Are we clear about any legal requirements on us to retain data for a certain period?
- Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?
- Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

## 8 TRAINING & EDUCATION

- Do we know about the levels of awareness of data protection in our organisation?
- Are our staff aware of their data protection responsibilities - including the need for confidentiality?
- Is data protection included as part of the training programme for our staff?

Please note this readiness assessment and its content are not exhaustive resources on GDPR policy and they should not be relied on as legal advice. Because legal information is not the same as legal advice – the application of law to one’s specific circumstances, we recommend consulting a lawyer if you need legal advice on how to interpret the legislation. This content is information for awareness purposes and to inspire you to review your current policies and practices.

## Questions about the GDPR?

Contact us to find out how Simpleview can help your company manage sensitive personal data in compliance with GDPR.

[info@simpleviewinc.com](mailto:info@simpleviewinc.com) or **520.575.1151**

[SIMPLEVIEWINC.COM](http://SIMPLEVIEWINC.COM)

simpleview 

