THE NEW EU DATA PROTECTION RULES

A GUIDE FOR RETAILERS

This guide was written by Joanna Lopatowska, adviser on consumer and e-commerce policy at EuroCommerce. It provides an outline of the provisions of the EU General Data Protection Regulation 2016, and gives informal guidance on the issues which retailers will need to address between now and 2018, when it comes into force.

Foreword

I am pleased to present this guide, which is aimed at offering an analysis and basic information about the 2016 General Data Protection Regulation, and providing some help to retailers in how to comply with the Regulation when it comes into force in 2018.

Personal data is a major and valuable asset for retailers in ensuring that they give the best service possible to consumers, in building customer loyalty and attracting new business. The interconnected world in which we live enables sophisticated use of data unimaginable only 10 years ago. In equal measure, the dangers of data being compromised, by intentional attacks or by inadvertent actions by employees or contractors, have also grown exponentially. The volume of personal data held on companies' databases, and privacy issues involved, has led to growing regulatory action at national and EU level, with penalties for breaching the regulations also becoming a major business risk. The new EU regulation imposes a number of additional obligations, but also brings some clarity and more uniform provisions in this important area.

It is said that knowledge is the best defence. This guide cannot be a substitute for professional advice, but we hope that its readers will find it useful in raising the right questions for them to ask, and some pointers towards actions that they need to take under the new regulation. One point that goes without saying – the earlier companies prepare for complying with the new rules, whether in dealing with data on customers or on their staff, the better they will be equipped to deal with the changes that the Regulation brings with it.

Christian Verschueren
Director-General

Abbreviations and symbols used in this guide

Directive
Data Protection Directive 95/46/EC

DPA
Data Protection Authority / Supervisory authority

DPO
Data Protection Officer

EU
European Union
The Data Protection Directive and the GDPR are both applicable in the European Economic Area (EEA), which comprises the 28 member states of the EU and Iceland, Lichtenstein and Norway.

GDPR or **Regulation**
General Data Protection Regulation 2016/679 of 27 April 2016

EuroCommerce comments on specific rules and requirements (in italic and blue).
The comments and examples provided are non-exhaustive. Regulatory guidance issued after the publication of this guide may provide additional examples, but also possibly interpretation of the GDPR.

Contents

10 key steps to compliance

1. Getting familiar with data protection

Companies should get to know, and be comfortable with, general data protection concepts and understand the role of their company as primarily responsible for the fairness, legality and security of the processing of personal data.

This concerns both big and small retailers, selling online and offline. A data protection reflex should become an integral part of each company's way of operating.

Many of the Regulation's main concepts and principles are the same as those in the Data Protection Directive. Therefore, if a company complies with the current obligations, the general approach to compliance and the way of doing things will remain valid under the GDPR.

However, there are new elements. Therefore, companies will have to do certain things for the first time and certain others differently.

2. General rules on transparency and legality

Companies should ensure that they are transparent about their use of personal data and the reasons for doing so. If a retailer collects personal data, it should have a relevant privacy notice in place.

Companies that have provided privacy notices under the Data Protection Directive should review them and update them by adding any missing details. Privacy policies should be robust and clear, be available on the website and be regularly updated.

Companies should identify all the legal reasons for which they process personal data. Companies will have to explain these in the privacy notice.

3. Customer privacy retail context

The GDPR does not provide for any specific rules on the processing of personal data in the retail context.

There are, and there will be, many questions on how the GDPR applies to the retail sector, which practices are permitted and may continue, and where retailers will need to change the way they handle data.

Many of these issues are currently unclear. What is clear is that, under the GDPR, retailers will need to explain, in a much clearer and accessible way, how they and their business partners are using customer data.

4. Individuals' rights

In addition to existing rights to access, rectification and deletion, individuals have new rights they can exercise, such as the right to data portability, and the right to erasure.

Companies should have procedures in place to handle individuals' requests in these areas.

5. Accountability

Companies should integrate privacy accountability in all their strategies and projects involving personal data.

Companies should have appropriate policies in place to ensure and demonstrate compliance. These policies should be regularly reviewed to make sure they are up-to-date.

Each company should develop a privacy culture and train staff to understand and fulfil their obligations. Awareness of the changes that are coming should be raised internally. Key management should be on board with changes, so that additional budget expenditure can be planned. Implementing the GDPR might be costly.

To be able to read the entire guide, please send us an email to timaru@eurocommerce.eu.