The EU Data Protection Overview

How marketers can understand compliance within the EU framework

Purpose of this Guide

This guide provides general direction about the following:

1. The current data protection laws governing the European Union (EU).
2. The proposed legal changes to European Union data-protection laws.

This guide will discuss how EU data protection laws affect online businesses that have a presence in the EU, including practical steps and best practices that online companies can take to demonstrate compliance and/or put themselves in a better position to comply with the new legislation once adoption and enforcement occurs.

THIS GUIDE IS NOT COUNTRY-SPECIFIC. Note that current EU data-protection laws are “Directives”, meaning they specify only minimum measures and can be uniquely interpreted and implemented by each Member State.

Although this has resulted in inconsistencies across the EU, most differences are related to administrative requirements and don’t have significant impact to overall compliance requirements.

However, two Member States – Germany and the United Kingdom – have stricter interpretations of certain sections of the laws, which set a higher bar for compliance.

Information specific to those Member States can be accessed at the following links:

- United Kingdom
- Germany

Legal Disclaimer

Contents

Introduction

On 25 January 2012, the European Commission (EC) published a proposal for a new Data Protection Regulation to replace the existing European Union (EU) Data Protection Directive.

The Regulation sets out a general data protection framework aimed at creating one EU-wide data protection law, thus unifying the patchwork of rules and guidelines currently in place across the EU Member States.

A majority of experts predict formal adoption by the European Parliament will occur between mid-2014 and early 2015. The Regulation will go into effect two years post-adoption; thus, organisations will need to be in full compliance between mid-2016 to early 2017, depending on when the law is approved.

For many, the impact will be profound, as most aspects of an organisation's compliance obligations will increase. In anticipation, online companies should begin taking steps to best ensure they are – and will remain – in compliance.

Background: EU Law Basics

Before delving into the changes and organisational ramifications and responsibilities inherent in the new law, it is important to generally understand the current EU Data Protection Directive.

A Brief History

Under its current name, the European Union has existed since 1993 and currently has 28 sovereign Member States.

In general, the EU's implementation of numerous "EU-wide" Directives has been done in piecemeal fashion due to the autonomy and independence of each Member State. This has resulted in a patchwork of differences depending on whether – and how – each Member State interprets the Directive's text.

Directive vs. Regulation

A **Directive** is a piece of EU legislation that is addressed to EU Member States. Once a Directive is passed at the EU level, each Member State must implement the Directive into its legal system, but it can do so in its own words. In other words, it is the law as interpreted by each Member State. Directives are used to bring different national laws in line with each other.

Conversely, a **Regulation** is the most direct form of EU law. As soon as a Regulation is passed, it automatically becomes the law as written, in each of the Member States. This means each Member State must implement the law in exactly the same way.

By adopting a Regulation for the new data protection issues, the EC intends to equip each of its Member States with the same basic legal instrument, applied uniformly. Theoretically, this should establish harmony and provide greater legal certainty across all Member States. The reality of adoption and implementation remains to be seen.

The Two EU Data Protection Laws Marketers Must Care About

The current European Union data protection legislation is based on several Directives, of which the following two are the most important and relevant:

1. **1995 Data Protection Directive** (Directive 95/46/EC). This requires protections for the processing and transfer of EU personal data.
2. **2009 "Cookie" Directive** (Directive 2009/136/EC). This requires informed consent before an organisation can access and/or store data on consumer devices. It covers all tracking technologies including cookies. It is also known as "ePrivacy Directive", "Citizen's Rights Directive", and "Telecoms Reform Directive".

These Directives are the basis for the data protections in all EU Member States and regulate the processing of personal data.

What follows is an overview of these two Directives, including the key requirements for compliance.

1995 Data Protection Directive (Directive 95/46/EC)

Overview

Directive 95/46/EC regulates the processing of personal data and the movement of such data within and outside of the European Union. It sets strict limits on the collection and use of personal data, and demands that each Member State set up an independent national body responsible for the protection of these data.

So what is "personal data"?

Personal data is any data consisting of information that relates to a natural person who can be directly or indirectly identified from that information. This includes identification numbers and any factors specific to physical, physiological, mental, economic, or social identity (e.g., name, age, gender, physical address, email address, bank statements, credit card numbers, and any behavioural information).

Processing of personal data means any operation that is performed on personal data, including collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

Scope

The 1995 Data Protection Directive applies to the following:

- Personal data processed within the EU.
- Personal data from EU citizens transferred to any foreign country.

The Directive applies to both electronic and paper files, whether transferred by automated or non-automated means.

What you need to understand:

Any website operator who collects information from EU citizens ***must comply*** with the 1995 Data Protection Directive, ***regardless*** of whether or not the company, organisation, or equipment is physically located in the EU.

Requirements for Compliance

Informed Consent

Informed consent refers to the data subject freely, specifically, and unambiguously giving consent to the processing of his or her personal data after being adequately informed of the data's collection and use.

In most countries, obtaining informed consent of the data subject at the time of personal data collection is sufficient; e.g., via an online form or other online opt-in process.

Special Case: Informed Consent from Minors

For some customers, questions may arise as to the reliability of consent obtained from minors.

The EU Directive does not address this issue directly, but Member States have specific rules that apply.

However, the issue of minor consent is addressed in the EC's 2012 proposal for a new Data Protection Regulation. Specifically:

> *"The processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian." Additionally, the proposal mentions that minors deserve extra protection because "they may be less aware of risks, consequences, safeguards, and their rights."*

Recommendation:

If your marketing efforts include the collection of consent from minors, it is recommended that you review the relevant local data protection laws that apply.

When Processing Personal Data is Permitted

There are six (6) conditions under which the processing of personal data – including transferring it to a third party or another country – is permitted.

1. **CONSENT** – The data subject has unambiguously and voluntarily given consent after being adequately informed.
2. **CONTRACT** – Processing of personal data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
3. **LEGAL OBLIGATIONS** – Processing of personal data is required by legal obligation.
4. **VITAL INTERESTS** – Processing of personal data is necessary to protect an interest that is essential for the data subject's life, for instance in the case of an emergency or accident.
5. **PUBLIC INTEREST** – Processing of personal data is necessary to perform tasks of public interest or tasks carried out by official authorities.
6. **LEGITIMATE INTEREST** – Processing of personal data is necessary for the purposes of legitimate interests pursued by the data controller, except where such interests are overridden by fundamental rights and freedoms of the data subject.

The Rules for Legally Processing Personal Data

If you meet one or more of the conditions that permit the processing of personal data, the following outlines the Directive's requirements for how personal data must be handled:

1. **FAIR AND LEGAL** – Personal data must be processed fairly and lawfully.
2. **PURPOSE-LIMITED** – Personal data must be collected only for explicit and legitimate purposes, must be used only for stated purpose(s) and for no other purpose(s), and must be relevant and not excessive in relation to the purpose for which the data are processed.
3. **RELEVANT** – Personal data must be adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed.
4. **ACCURATE** – Personal data must be accurate and, where necessary, kept up to date; data controllers must provide reasonable measures for subjects to correct, erase, or block incorrect data.

5. **TIME-LIMITED** – Personal data must not be kept longer than is necessary for the purposes for which the data were collected or for which they are further processed.

The Rights of Data Subjects

In addition to outlining how and when personal data may be legally processed, the Directive also establishes the rights of data subjects, which are:

1. **RIGHT OF ACCESS** – Data subjects have the right to obtain information regarding:
   - Whether their personal data are being processed, and
   - The content and source of any personal data being processed, and
   - The purpose of such processing.
2. **RIGHT TO CORRECT** – Data subjects have the right to correct, erase, or block the transfer of inaccurate or incomplete data.
3. **RIGHT TO OBJECT** – Data subjects have the right to:
   - Object at any time to having their personal data processed, save where otherwise necessary or required by national legislation, and
   - Object to the processing of personal data that the data controller (see "What is a Data Controller?", this page) anticipates using for purposes of direct marketing.

Obligations of Data Controllers

What is a "Data Controller"?

Data controllers are the people or organisational body that determines the purpose and means of data processing, both in the public and private sectors. For example, a medical practitioner would usually be the data controller of the data processed on her clients; a company would be the controller of the data processed on its clients and employees.

In addition to specifying how and when personal data may be processed, the Directive imposes other obligations on data controllers.

Notice to Data Subjects

Data controllers must provide the data subject with the following information:

1. The identity of the data controller.
2. The purpose of the data processing.
3. The recipients or "categories of recipients" of the subject's data.
4. Whether providing information is obligatory or voluntary (including an explanation of the consequences of failure to provide the information).
5. The existence of the right to access and correct personal data.

Notice to Data Protection Authorities

Data controllers must notify the local supervisory authorities in each applicable Member State before commencing any automated processing of personal data. (Note that national Data Protection Authorities (DPAs) have been established in almost all EU Member States.)

Depending on the Member State, this notification may be substituted by the appointment of a personal data protection official (DPO). This person ensures, in an independent manner, the internal application of data protection law and keeps a register of processing operations carried out by the controller.

For more information, visit:

- European Data Protection Supervisor website
- List of EU Member State DPAs
- List of DPOs by EU Member State

Transferring Personal Data to Non-EU Countries

When transferring data within the EU and/or the associated countries of the European Economic Area (EEA) – currently Norway, Liechtenstein, and Iceland – no additional restrictions apply.

However, the Directive expressly prohibits the transfer of personal data to non-EU/EEA countries that do not ensure an "adequate level of protection".

Here's what that means:

Adequate Level of Protection

Determinations regarding which countries provide the requisite level of protection are made by the EC with recommendations from a Working Party. To date, the EC has identified only Argentina, Canada, Guernsey, the Isle of Man, and Switzerland as providing adequate protection.

Note the United States is absent from this list.

Safe Harbor (Adequate Level of Protection for United States Only)

In 2000, the EU and the United States Department of Commerce reached an agreement that permits the transfer of personal data from the EU to U.S.-based organisations that publicly certify themselves to be a "Safe Harbor", provided they comply with all of the following privacy principles:

1. **NOTICE** – Let consumers know what you do with the data you collect.
2. **CHOICE** – Give consumers the ability to opt-out of data sharing with third parties.
3. **ONWARD TRANSFER** – Third parties you share consumer data with must also comply with Safe Harbor (or EU Directive) principles.
4. **ACCESS** – Allow consumers to access and correct data you've collected about them.
5. **SECURITY** – Take reasonable steps to protect the personal data collected.
6. **DATA INTEGRITY** – Ensure the personal data collected are relevant and accurate.
7. **ENFORCEMENT** – Offer consumers an independent recourse mechanism for privacy disputes.

To become certified for Safe Harbor status, a U.S.-based organisation must provide specific information to the U.S. Department of Commerce on an annual basis.

NOTE: Germany adopts a stricter interpretation of Safe Harbor compliance than do other Member States. However, **the EU has agreed that Safe Harbor is an adequate level of cross-border compliance**. To read more, please see Germany's additional legal requirements.

Act-On Certification:

Act-On has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement.

To learn more about the Safe Harbor Treaty, and to view Act-On's certification, please visit http://www.export.gov/safeharbor

Act-On has earned Trusted Cloud and EU Safe Harbor Practices certifications by TRUSTe, the world's largest privacy seal program. For more information, please visit www.truste.com.

Processing of Sensitive Personal Data

In principle, sensitive personal data cannot be collected or processed. The Directive defines sensitive personal data as *"data which are capable by their nature of infringing fundamental freedoms or privacy."* This includes but is not limited to:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or affiliations
- Trade union memberships
- Medical records and health
- Sex life

Collection of sensitive data is tolerated only under very specific circumstances. Examples include the data subject's explicit consent, processing of data mandated by employment law, and where it may be impossible for the data subject to consent (e.g., the victim of an accident).

Recommendation:

If you choose and/or require collection of sensitive data, it is highly recommended that you do a detailed review of the requirements of each Member State to ensure you are in compliance.

Enforcement

Enforcement varies from country to country because there is no central EU data protection agency. Thus, data protection laws are enforced by the data protection authorities of the individual Member States and through the European Data Protection Supervisor.

2009 "Cookie" Directive (Directive 2009/136/EC

Overview

Directive 2009/136/EC amends Article 5(3) of the EU e-Privacy Directive (Directive 2002/58/EC), adding new rules that require online service providers to obtain prior, informed consent from users for the use of any online tracking technologies.

It gives control to EU citizens as to when their online behaviour can be tracked. For marketing organisations, this has widespread impact.

Scope

The Directive must be implemented by all EU Member States; however, it does not specify how "prior informed consent" needs to be achieved. Thus, each Member State has leeway in how to enforce this legislation.

Requirements for Compliance

Data controllers must comply with the following, which closely align with those found in Directive 95/46/EC:

- Inform consumers their data are being processed.
- Get consumer consent prior to storing or accessing information on the consumer's computer or other device.
- Give consumers access to their data to correct it or delete it.
- Use consumer data only for disclosed purposes.

Important:

Data cannot be transferred outside of the EU unless these data protection standards are met.

How This Impacts Marketers

IF: You use cookies or other tracking technology to store or access information from EU citizens on their computers or devices ...

THEN: You must comply and get permission before cookies and/or other tracking technologies are placed or used.

Examples of Tracking Technology Uses

If your company has a website, it more than likely uses multiple types of tracking. For purposes of illustration, examples include (but are not limited to):

- Analytics
- Targeted advertising
- Site personalization
- Shopping cart management
- Visitor preferences
- Web beacons
- Mobile apps
- Email

Exception

The Directive specifies the following exception to acquiring prior informed consent for using tracking technologies:

Only if "technical storage or access is strictly necessary for the legitimate purpose of enabling a specific service explicitly requested by the subscriber or user".

Specific exceptions are:

- Secure login session cookie
- Shopping basket cookie
- Security cookie (to comply with EU law)

Practical Steps to Compliance

1. Identify stakeholders within your organisation and create a taskforce.
2. Conduct a comprehensive audit of your existing tracking mechanisms on all websites and/or online properties.
3. Prepare for a workable opt-in solution in the EU, including the creation and prominent posting of your cookie policy.

Opt-in Consent Model Examples

There are several methods being deployed by companies to ensure compliance with the Directive. These include:

- Updating the cookie policy only, with a link on the website directing visitors to the new information.
- **Implied Consent** – Providing notice about cookie use (e.g., via a pop-up or header bar), including opt-out action required from the user.
- **Explicit Consent** – Providing notice with opt-in action required from the user.

Country-Specific Requirements

Although there are many differences from country to country as it relates to data protection laws, the overview and solutions provided in this guide will be sufficient to cover legal privacy requirements in most Member States.

However, Germany and the United Kingdom have adopted additional and/or stricter guidelines for compliance.

If you have business presence in either of these countries, additional laws and requirements can be found at the links below.

- Germany
- United Kingdom

Resources

- European Commission website
- Full text of 1995 Data Protection Directive (Directive 95/46/EC)
- European Data Protection Supervisor information
- Full text of 2009 Cookie Directive (Directive 2009/136/EC)
- Safe Harbor Program
- Germany – Additional Legal Requirements
- United Kingdom – Additional Legal Requirements
- Protection of Minors: Age of Consent in EU Member States
- National Data Protection Laws in EU Member States

Proposed Changes
New EU Data Protection Regulation

As presented in the Introduction to this guide, a sweeping Regulation has been proposed that, if adopted, will create a single EU-wide data protection law.

The new Regulation aims at unifying, strengthening, and simplifying the current patchwork of data-protection Directives currently in place. The belief is that it will remove fragmentation and administrative burdens, result in cost savings, and reinforce consumer confidence in online services (which is projected to boost growth, jobs, and innovation).

Here's what you need to know to prepare for compliance.

What's Changing?

Key changes in the proposed reform are:

Basic Principles of Data Processing

- When informed consent is required for data processing, it will have to be given **explicitly**, rather than implicitly or assumptively.
- EU rules will **apply to non-EU companies** that offer goods or services in the EU or monitor the online behaviour of EU citizens.
- **New definitions** will be supplied to cover technological advancements such as "genetic data" and "biometric data".
- Explicit **parental consent** is required prior to processing the data of a child under age 13.
- Companies established in more than one EU country will be monitored by **one single data processing authority (DPA)**, rather than separate authorities per country.

Rights of Data Subjects

- A **"right to be forgotten"** allowing individuals to have all personal data that business holds on them deleted, including photos and public links to (or copies of) personal data that can be found anywhere on the Internet. (Note this may change to the **"right of erasure"**, which will strengthen the edict because it would empower data subjects with the right to have their personal data permanently erased. Permanent erasure is much more potent than mere deletion, because deleted data often can be restored; permanently erased data cannot.)
- A right to have personal data corrected or deleted **free of charge** when said data are processed and used for direct marketing purposes.
- A right to access one's personal data, including the **right of data portability**; i.e., ability to transfer personal data from one service provider to another.

Obligations on Controllers

- Data controller obligations will be **expanded to cover data processors**.
- Unnecessary administrative burdens will be **removed**.
- **Responsibility and accountability** for those processing personal data will be increased, including documentation and data security requirements.
- Concept of **"data protection by design"** will be formalized.
- Reporting of **data breaches** must be done "without undue delay" – usually within 24 hours.

Penalties for Breaches

A breach of the new data protection rules could result in **a fine of up to 5% of the global annual turnover** (i.e., the gross amount of revenue received in a 12-month period) of a company. Fines will be imposed by the Data Protection Authority.

Get More Information

Act-On will update this guide from time to time and/or as appropriate. However, please familiarise yourself with the latest information on sites including:

- For policy fact sheets: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
- International Association of Privacy Professionals: https://www.privacyassociation.org/

Supplement A:

Data Protection Law in the UK

Purpose of this Supplement

This supplement to the EU Data Protection Requirements guide is specific to the **United Kingdom (UK)**, providing a high-level overview of the EU privacy laws sections where the UK has adopted additional and/or stricter requirements. It is not intended to replace the EU Data Protection Requirements guide.

Legal Disclaimer

Note that this guide provides general information about basic principles of data protection law in the EU. It does not constitute legal advice, and Act-On Software does not accept any liability regarding its completeness, accuracy, or relevance.

Have additional questions?

For non-legal requests or questions concerning EU compliance, Member State compliance, or configuring Act-On Software for compliance, contact your Customer Success Manager for assistance.

Supplement A: Data Protection Law in the UK

General Law: UK Privacy and Data Protection Framework

There are two main sets of laws in the UK that cover the activities of direct marketers:

1. **Data Protection Act 1998.** This covers protection for the processing and transfer of UK citizens' personal data.
2. **Privacy and Electronic Communications Regulations 2003.** This covers informed consent, spam, and all tracking technologies including cookies.

These laws are currently used to implement the requirements set forth by the EU Data Protection Directive (95/46/EC) and the "Cookie" Directive (2009/136/EC), respectively.

Data Protection Act 1998

The Data Protection Act 1998 (DPA) covers personal data about any living and identifiable UK citizen, where the personal data are:

- Held or intended to be held on computers.
- Held in a "relevant filing system" (e.g., diaries used to support commercial activities, such as a salesman's physical address book).

Additionally, the DPA covers more than e-commerce businesses and is not restricted to buying and selling online; it also covers most e-marketing activities (referred to as "information society services"), regardless of message or purpose. The UK's Department of Trade and Industry says:

"The requirement for an information society service to be 'normally provided for remuneration' does not restrict its scope to services giving rise to buying and selling online. It also covers services (insofar as they represent an economic activity) that are not directly remunerated by those who receive them, such as those offering online information or commercial communications (e.g. adverts) or providing tools allowing for search, access and retrieval of data."

The DPA does not specifically cover "privacy".
For this and other reasons, the DPA has been refined by subsequent legislation, including the Privacy and Electronic Communications Regulations (see next section).

Privacy and Electronic Communications Regulations 2003

Also known as the Electronic Commerce Directive (EC Directive) or the UK's "Cookie Law", the Privacy and Electronic Communications Regulations (PECR) are the UK's main laws for dealing with spam and online consent, including:

1. Sending electronic marketing messages by:
   - Telephone calls (telemarketing or automated)
   - Fax
   - Email
   - Text, picture, or video message
   - Viral marketing
2. Using cookies and/or similar technologies for storing information on a user's equipment, such as their computer or mobile device.

Supplement A: Data Protection Law in the UK

Law Enforcement: the Information Commissioner's Office

Interpretation, oversight, and enforcement of UK data protection laws is managed by the Information Commissioner's Office (ICO), an independent authority in the UK that promotes:

- Openness of official information
- Protection of private information

According to its website, the ICO does this *"by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action when the law is broken."*

The ICO scope includes the DPA and PECR.

What the ICO has power to do:

There are a number of tools available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use, and keep personal information about UK citizens.

They are:

- Criminal prosecution
- Non-criminal enforcement
- Compliance audit
- Monetary penalty of up to £500,000

ICO Enforcement Approach: Regulatory Action

The ICO exercises its powers via Regulatory Action. The ICO's Regulatory Action Policy states:

> *"The ICO has powers to change the behaviour of organisations and individuals that collect, use, and keep personal information. These powers are designed to promote compliance with the Act [DPA], PECR, and related laws. They include criminal prosecution, civil monetary penalties, non-criminal enforcement and, in some circumstances, audit. Regulatory action is the term used to describe the exercise of these powers."*

Reasons for a Regulatory Action

According to ICO policy, it uses a "selective approach to initiating and pursuing regulatory action." Its decision is *"driven by concerns about significant actual or potential detriment caused by non-compliance with data protection principles, the PECR, or other relevant legal requirements."*

Common drivers of regulatory action are (but not limited to):

- Issues of general public concern (including those raised in the media).
- Concerns that arise because of the novel or intrusive nature of particular activities.
- Concerns that are raised with the ICO via complaints.
- Concerns that become apparent through other ICO activities.

Supplement A: Data Protection Law in the UK

What Do Marketers Need to Know?

The majority of the DPA and PECR closely align with the EU Data Protection Directive and EU Cookie Directive, respectively. Thus, compliance with the EU laws is highly recommended.

However, there are areas where the UK imposes additional and/or stricter requirements than those in the EU laws. These areas are:

- Data controller registration
- ICO Guidance for direct marketers
- Penalties for breach

Data Controller Registration

The DPA requires every organisation that processes personal information on UK citizens to register with the ICO, unless they are exempt. Failure to do so is a criminal offence.

Exemptions from DPA rules can be "complete" or "partial", with the ICO being the final arbiter of whether or not data controllers must register. To find out whether your organisation is required to register, visit the ICO Register/Notify website, which offers an online assessment tool.

Currently there are more than 370,000 data controllers registered with the ICO. The ICO publishes the name and address of these data controllers, as well as a description of the kind of processing they do.

For most organisations, the cost is £35 each year.

ICO Guidance for Direct Marketers

The ICO clarifies existing obligations under the DPA and/or the PECR using an instrument called "Guidance". On 10 September 2013, the ICO issued a new Guidance on direct marketing, offering further explanations about how the DPA and PECR apply to direct marketing in the UK.

Consent is a key focus of the Guidance, aligning the historically looser UK requirements with those of the EU. Key tenets include:

- Organisations will need to obtain "*extremely clear and specific*" consent in order to send direct marketing communications, and can no longer rely on implied consent "*as a euphemism for ignoring the need for consent, or assuming everyone consents unless they complain*."
- Organisations should keep clear records of exactly what an individual has consented to and, in particular, they should record the date of the consent, the method of consent, who obtained consent, and exactly what information was provided to the person consenting.

The ICO guidance is not legally binding...but:

It is highly recommended that you comply.

Reason: The Guidance reflects the ICO's interpretation of the DPA and PECR requirements, and is a good indication of how the ICO is likely to enforce them.

Supplement A: Data Protection Law in the UK

- When tick-boxes are used to obtain consent, the boxes should seek opt-in – rather than opt-out – consent.
- Organisations should maintain a "suppression list" of people who have opted out or otherwise told that organisation directly that they do not want to receive marketing.
- With purchased email marketing lists, "*indirect consent* [i.e., consent obtained by third parties] *is unlikely to be sufficient*."
- Under the PECR, the rules for consent required for emails also apply to any electronically stored messages, including texts and some social networking messages. "*The rules [also] apply to viral marketing,*" the ICO said in its Guidance. "*[O]rganisations will still need consent even if they do not send the messages themselves, but instead instigate others to send or forward them*."

To assist, the ICO has made available a detailed overview of the Guidance, as well as a short checklist.

Penalties for Breach

The ICO has the power to issue monetary penalty notices of up to £500,000 to organisations that are in serious breach of the DPA or PECR.

Supplement A: Data Protection Law in the UK

Whose Laws Apply?

For an organisation that has physical presence in the EU (including a brick-and-mortar location and/or a server), it is highly recommended that it comply with the EU Data Protection Requirements.

If an organisation has physical presence ONLY in the UK, the PECR applies a "country of origin" principle. According to international law firm, Pincent Masons, this means that:

> *"... as long as a UK business complies with the provisions of the [PECR], it can 'ignore' the laws of other Member States that touch upon the same subject matter."*

However, this ignoring of other Member States' laws is not absolute. Pincent Masons continues: *"A UK business cannot, however, escape the terms of the [PECR] simply by locating its servers outside the UK. The [PECR] look[s] at where a business is established, not where its equipment is based."*

Supplement A: Data Protection Law in the UK

Resources

- ICO website
  - ICO Data Protection Regulatory Action Policy (Aug 2013) (PDF)
  - ICO Guide to Data Protection (PDF)
  - ICO Guidance on Direct Marketing (PDF)
  - ICO Direct Marketing Checklist (PDF)
- UK Data Protection Act 1998
- UK Privacy and Electronic Communications Regulations
- Direct Marketing Association UK (DMA-UK)
- European Commission website

Supplement B:

Data Protection Law in Germany

Purpose of this Supplement

This supplement to the EU Data Protection Requirements guide is specific to **Germany**, providing a high-level overview of the EU privacy laws sections where Germany has adopted stricter requirements. It is not intended to replace the EU Data Protection Requirements guide.

Legal Disclaimer

Note that this guide provides general information about basic principles of data protection law in the EU. It does not constitute legal advice, and Act-On Software does not accept any liability regarding its completeness, accuracy, or relevance.

Have additional questions?

For non-legal requests or questions concerning EU compliance, Member State compliance, or configuring Act-On Software for compliance, contact your Customer Success Manager for assistance.

Supplement B: Data Protection Law in Germany

General Law: Areas Covered by Stricter Amendments

The main legal source of data protection in Germany is the Federal Data Protection Act (Bundesdatenschutzgesetz) (BDSG), which implements the requirements set forth by the EU Data Protection Directive 95/46/EC.

On 1 September 2009, Germany amended the BDSG with stricter requirements that cover the following business-specific issues:

- Marketing
- Security breach notification
- Service provider contracts
- Employee data protections
- New powers for data protection authorities
- Increased fines for violations

Supplement B: Data Protection Law in Germany

When Does German Law Apply?

The BDSG applies to:

- German data controllers and processors (private and public bodies).
- A German branch of a data controller located in the European Economic Area (EEA*) that collects, processes, and uses personal data from German citizens.
- All global data controllers – EXCEPT those that are located within the EEA – that collect, process, and use personal data from German citizens.

**EEA countries include the EU Member States, plus three non-EU countries that are members of the EFTA (European Free Trade Association): Norway, Iceland, and Liechtenstein.*

Supplement B: Data Protection Law in Germany

How German Law Affects Marketers

The majority of amendments to the BDSG closely align with the EU Data Protection Directive; thus, compliance with the EU laws is highly recommended.

However, there are specific areas where Germany imposes stricter requirements than those in the EU laws. These areas are:

- Data controller obligations
- Obtaining informed consent
- Sanctions and penalties

Variations in Enforcement:

No single data protection authority exists in Germany. Rather, each of the country's 16 separate states (Länder) can interpret and enforce the BDSG independently.

Supplement B: Data Protection Law in Germany

Data Controller Obligations

Notifying German Authorities Prior to Processing Data

In theory, the BDSG requires notification prior to the collection, processing, and use of personal data. However, in practice, this requirement is waived if the data controller has appointed a data protection officer (DPO) because these appointments are mandatory for all companies that either:

- Have 10 or more persons regularly involved in the automated data processing, or
- Process sensitive personal data.

Since most Act-On customers (i.e., data controllers) meet the criteria for appointing a DPO, no further notification is required. The appointed DPO will be responsible for – and have the authority of – ensuring internal compliance to BDSG requirements.

For Act-On customers that do not meet the criteria for appointing a DPO, Länder authorities will need to be notified before commencement of any data processing activities. Notification is an informal process in Germany; thus, data controllers must contact the German data protection authorities in their respective Länder for instruction.

Contracts between Data Controllers and Their Service Providers

The BDSG requires contracts to be in place between data controllers (i.e., companies collecting data) and their service providers (i.e., data processors such as Act-On).

Contracts must specify the following:

- Scope, purpose, and categories of the data processing
- Technical and organizational security measures
- Data processor obligations, particularly in relation to monitoring
- Subcontracting rights
- Data controller rights to audit, monitor, and/or issue instruction to the processor
- Data erasure and blocking policies
- Return of storage media
- Disposal
- Rules applicable if the processor or its employees violate:
  - provisions relating to the protection of personal data, or
  - terms specified by the controller, which are subject to the obligation to notify.

This requirement affects all contracts between German entities, as well as contracts between foreign service providers and their German customers.

Supplement B: Data Protection Law in Germany

Security Breach Notification

Section 42 of the BDSG specifically requires data controllers to comply with comprehensive breach notification requirements if BOTH of the following occur:

- Particularly sensitive data (including bank or credit card data, telecommunications and/or online collected data, data related to criminal offences, and personal data subject to professional or official confidentiality) are abused or lost, and a third party acquires knowledge of the contents.
- There is a serious threat of interference with the interests of the relevant data subjects.

When breach notification is required, data controllers must inform the appropriate data protection authorities and the affected data subjects without delay (a) after appropriate measures have been taken to secure the data and (b) once criminal prosecution will no longer be affected.

Where notification to individuals would be disproportionately burdensome, particularly where a large number of individuals are affected, notice must be provided to the general public by means that would provide adequate information exposure.

Encryption and Tokenization as Viable Security Measures:

The BDSG explicitly refers to encryption and tokenization technologies as being appropriate for access control and safeguarding data transmission, as long as they reflect the "Stand der Technik" – state-of-the-art technology.

The BDSG directly aligns with the EU Data Privacy laws for data transfer; namely, transferring data from German companies to foreign companies is not a problem as long as these companies are located in the EEA (the EU plus EFTA countries).

Germany's Requirement

German companies that transfer data to U.S.-based companies must now observe the following procedure: If data are exported from Germany to the U.S., then the data exporters are obligated to *actively review compliance* with the minimum standards of data protection laws, even if the U.S. company receiving data has agreed to the Safe Harbor Treaty.

Supplement B: Data Protection Law in Germany

Here is the explanation of what *active review* means:

A: Written documentation of agreement to the Safe Harbor Treaty must be presented.

- Written documentation must be presented to the German data exporter stating that the company has agreed to the Safe Harbor Treaty.
- This documentation may not be older than seven years and must include the substantial obligations of the Safe Harbor Treaty.
- Receipt of this confirmation should be carefully documented because the responsible party is obligated to present it at the request of data protection officials.

B: Verification of compliance with notification duties must be obtained.

- The German data exporter must obtain verification from the potential data recipient that the data recipient has complied with notification duties to the affected party that have been established in the Safe Harbor Treaty itself.
- The company must notify the subjects affected by the data transfer about the purpose for which data will be collected, how they can contact the organization in the event of any questions or complaints, what types of third parties the data will be shared with, and what means are available to private individuals so they can limit the use and dissemination of the data.

RECOMMENDATION: Companies should ensure to meet these requirements. Germany's Institute for IT Law (IITR) reports that data protection regulators at the Länder-level are adhering to these very closely.

Act-On Certification:

Act-On has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement.

To learn more about the Safe Harbor Treaty, and to view Act-On's certification, please visit http://www.export.gov/safeharbor

Act-On has earned Trusted Cloud and EU Safe Harbor Practices certifications by TRUSTe, the world's largest privacy seal program. For more information, please visit www.truste.com.

Supplement B: Data Protection Law in Germany

Obtaining Informed Consent

In Germany, all consent for electronic marketing communications must be "explicit" as it relates to using tracking devices (including cookies), as well as sending electronic communications (email and SMS).

Below are the key areas marketers must understand.

Requirements for Obtaining Valid Consent

In an online environment, the following must be met in order for consent to be valid:

- The wording of the consent is made distinguishable in its appearance by being in bold letters, framed, or otherwise clearly emphasized.
- Text of the consent is in plain language and easy for the individual to understand.
- Consent is given by the user unambiguously, deliberately, and expressly, and must be given prior to the collection of personal data.
- The type of data collected and how it is collected must be disclosed.
- The purpose for processing the data must be disclosed. (Consent will only be valid for processing activities that are covered by the purpose(s) identified to the individual at the time of consent.)
- Consent cannot be modified without detection.
- The data controller can be identified.
- Information about the consequences of not consenting are provided (e.g., the service may have limited functionality, etc.).
- A brief explanation of the rights of the user must be provided.
- User consent is recorded.
- A record of the consent can be obtained by the user on request and at any time.

Supplement B: Data Protection Law in Germany

Sanctions and Penalties

Data protection laws are actively enforced in Germany. Violations are subject to the following:

- A maximum €300,000 fine for administrative offences.
- Imprisonment of up to two years or a fine, depending on the seriousness of the violation (e.g., in the case of wilful behaviour or if conducted in exchange for financial benefit).
- Reputation damages, which are not direct financial damages but damages caused, for example, by negative press. (Recent data protection scandals showed that reputation damages are usually quite severe if data protection breaches become public.)
- Confiscation by the data protection authority of any profit and/or benefit derived from a violation.

Supplement B: Data Protection Law in Germany

Additional Resources

- German Data Protection Authority website
- European Commission website

Have Questions?

For non-legal requests or questions concerning EU compliance, Member State compliance, or configuring Act-On Software for compliance, contact your Customer Success Manager for assistance.

David Fowler, Chief Privacy and Deliverability Officer, Act-On Software

David Fowler serves as Act-On Software's Chief Privacy and Deliverability officer. He has over 20 years of international experience in the marketing industry, including ten years strictly focused on the issues associated with internet privacy compliance, email marketing, deliverability, and digital marketing.

Mr. Fowler is a seasoned speaker and email deliverability consultant with national and international engagements that include: International Association of Privacy Professionals (IAPP), Federal Trade Commission (FTC), InBox East and West, Inbox/Outbox - London, American Marketing Association, Messaging and Anti Abuse Working Group (MAAWG) - U.S. and EU, TRUSTe, Privacy and American Business and the Email Insider Summit.

About Act-On Software

Act-On is a leading provider of integrated marketing automation software, helping companies to tie inbound, outbound and nurturing programs together – across email, web, mobile, and social. Our customers achieve superior Return on Marketing Investment by using sophisticated behavioral data to increase engagement throughout the customer lifecycle, reduce the cost of customer acquisition, and strengthen customer loyalty. Act-On's fresh approach to marketing automation gives its users full functionality without the complexity other systems impose, and makes campaign creation and program execution easier and faster. Act-On offers a best-in-class professional services team, around the clock customer support, and the APEX ecosystem of partners to provide clients with the tools they need to achieve marketing success.

+1 (877) 530 1555
www.act-on.com