BASDA
The Voice of UK Business Software

www.basda.org

10 things to consider to ensure GDPR Compliance

GDPR (General Data Protection Regulation) was mandated by the European Union and was enshrined in UK Law on 25th May 2018. It goes much further than the original UK Data Protection (of individuals) provisions applying before that date and lays down severe penalties for the officers (Directors, Owners and sometimes Managers) of businesses that do not comply.

Fines can be as high as 4% of turnover. Widely reported data breaches have seen British Airways and Marriott Hotels handed fines totalling £300m.

GDPR exists to restrict the amount of information held by an individual or business (including sole traders) about individuals as being wholly and primarily necessary for the conduct of business. Such holders of this data are described as **Data Controllers**. The UK Information Commissioner also identifies the distinct roles of **Joint Controllers** and **Data Processors**. For more detail on the provisions of GDPR visit the Information Commissioner's Office **www.ico.org.uk**

GDPR affects BASDA (The Business Applications Software Developers Association) members both as companies which hold data, for example on their employees and customers, and as providers of business software which enables organisations to hold and process data on individuals.

Historically almost any information could be held and maintained so long as it was not published. Now any information held about an individual must be fit for purpose (for example, to fulfill any obligations associated with providing a service) and as importantly, must be provided, if requested, to an individual. Below are 10 things from BASDA for a business to consider relating to GDPR.

1 I am a Data Controller. Do I have to register my activities with the GDPR Registrar?

Yes. Data Controllers that hold, maintain and process personal data need to pay a data protection fee to the Information Commissioner's Office (ICO), unless they are exempt. Currently the fee ranges between £40.00 and £2,500.

2 Who exactly is covered by the provisions of GDPR?

Any individual that believes a Data Controller holds personal data about themselves. This includes employees; client staff; supplier staff; prospective client and supplier staff; people who are sent marketing information about own and third-party products and services etc.

3 What are my obligations in respect of accessing data I hold?

Individuals have the statutory right to access any personal data a Data Controller may hold about them. This is commonly referred to as 'subject access'. A request can be made for subject access for full disclosure of all information held by a Data Controller about themselves verbally or in writing and the business has one month to respond. Not responding with full disclosure carries severe penalties for the officers of the business. A fee is not normally chargeable to an individual who makes a request under the provisions of GDPR.

4 What is the information that I may be required to deliver if I receive a request for subject access?

Any information that relates to the subject access, whether held in 'electronic form' (to be delivered in paper form), audio recordings, video recordings (then direct copies of these last two) or paper. 'Electronic form' includes data held in databases, files (word proccessed, spread sheets etc.) and emails (both business and private).

5 How do I ensure internal compliance?

The first step is to ensure that all internal Policies and Procedures make it clear to all staff (and where used, contractors) that only information relevant to the needs of the business are to be recorded about people whom there may be contact with. Moreover, if the servers of the business are used to access (by people within the business) personal emails or social media sites (Facebook, Twitter etc.) it should be made clear that the business has the obligation to deliver any related material from those sources upon receiving a request for subject access. A safe course of action is to prohibit access to personal email and social media sites using the business servers. However, a failsafe is to ensure all staff and contractors know that if they have unfettered access to such data to ensure they comply with the provisions of GDPR.

6 I have received a verbal request for access – what do I do?

Although it is preferred that all requests are received in writing it is reasonable for an employee to request information being held about themselves by an employer. It is therefore essential to document clearly in the Policies and Procedures of the Data Controller how to register such a verbal request and ensure that information is delivered appropriately.

7 Why are emails covered by the provisions of the legislation?

Too often emails (or similar communications) are used as a means of expressing views (both good and bad) about an individual that has little or nothing to do with business. These views, in addition to holding personal data, could be defamatory in nature (a matter for the Policies & Procedures) and if about a fellow colleague (who can seek access under the provisions of GDPR) could leave a business open to employment litigation. Where a request has been received for subject access it is necessary to redact mention of any other personal data that is not specific to the request, i.e. that belongs to another person. Delivering personal data for another person when responding to subject access is an offence under the provisions of GDPR.

8 I deliver software for installation by clients. Does this make me a Data Controller of data they may hold?

If you deliver software solutions (normally under licence) that you subsequently maintain and offer remote diagnostic services for, where such remote services may include accessing information held on a database that includes personal information, you are conceivably operating as a Data Controller. It is therefore important to review existing support/ maintenance agreements and include wording such as:
"If we are requested in writing to access and perhaps modify the contents of a data base or related files that contain personal data we will document any changes that are made and pass that full documentation to the client/licensee. Once that information has been passed to the client/licensee we will delete all references and temporary copies from our own systems. This will preserve our role as being that of a Data Processor, not a Data Controller."

9 I offer Software as a Service (SaaS) solutions where I host data being maintained by clients. Does this make me a Data Controller?

Typically offering SaaS implies that underlying databases and related files that may contain personal information are under your direct control. In this event it would be worth ensuring that contracts with users of the service include wording like:
'We are operating as a Data Processor in providing the services described herein. If we are requested in writing to access and perhaps modify the contents of a database or related files that contain personal data we will document any changes that are made and pass that full documentation to the client/licensee. Once that information has been passed to the client/licensee we will delete all references and temporary copies from our own systems. This will preserve our role as being that of a Data Processor, not a Data Controller."

10 What if our servers are hacked and data is copied (stolen)?

The Information Commissioner makes it clear that a Data Controller is responsible for the security of any personal data that it holds. The fact that a server is hacked, or an employee takes a copy of personal data is no excuse and still leaves the Data Controller (especially its Officers) liable under the provisions of GDPR. Care should be taken to ensure that even the copying of one individual's data is not permitted unless for the sole legitimate purpose of the Data Controller. Copying is not limited to delivering the data over communication services – it includes copying to portable storage such as USB sticks or SIM cards.

About BASDA

BASDA is the trade association which is the voice of UK business software. BASDA doesn't promote any specific software nor engage in any customer commercial discussions. BASDA focuses on common issues, needs and regulatory matters which affect members (and their customers). BASDA members provide a wide range of solutions for organisations of all sizes. To find out more, visit **www.basda.org**
BASDA members include:

BASDA
The Voice of UK Business Software

Published by:
BASDA – Business Application Software Developers' Association
PO Box 118, Dursley, Gloucestershire GL11 9BU
T +44 (0)1494 868030 **E** marketing@basda.org