EU General Data Protection Regulation

This briefing provides an overview of the key changes introduced by the EU’s General Data Protection Regulation (the “GDPR”), which will have extra-territorial effect in the Channel Islands in relation to the personal data of EU citizens, and the provisions of which will also be introduced into Jersey and Guernsey domestic law. The GDPR comes into force in May 2018.

Introduction

Data protection laws control how information about people is used by organisations.

Data that relate to living individuals are a commodity. Combating theft, leaks or other misuse of data is a growing challenge. Laws that set minimum standards of behaviour regarding the use of personal data must endeavour to keep pace with technologies which are evolving rapidly.

Jersey has had data protection laws in place since 1987. The current legislation is the Data Protection (Jersey) Law 2005 which, together with numerous regulations, reflect the EU and UK laws that inspired them. Guernsey’s current legislation is the Data Protection (Bailiwick of Guernsey) Law 2001, as amended. Both islands’ existing domestic legislation is considered by the EU to provide an equivalent (“adequate”) level of protection to individuals (“data subjects”) to the EU Directive 95/46/EC on which it is based.

Change

In 2012, proposals were put forward within the EU to overhaul its data protection regime, beginning a four year consultation process involving the EU institutions, businesses, civil society and stakeholders. In April 2016, the GDPR was adopted by the European Council. As an EU Regulation, it will have direct effect in all EU Member States - including the United Kingdom pre-Brexit - in May 2018.

Relevance of GDPR in the Channel Islands

The GDPR has extra-territorial effect. It applies not only to entities based in the EU, but to any entity offering goods and services in the EU. Businesses will be responsible for data protection compliance wherever they are based as long as they are processing EU citizens’ personal data.

Jersey and Guernsey are also proposing to introduce new domestic legislation (replacing their existing laws) which will match the essential safeguards of data subjects and their personal data as set out in the GDPR, so that their current “adequate” status is maintained, permitting the free transfer of data between the Channel Islands and EU Member States. The States of Jersey approved drafting instructions for a new law in February 2017 and the States of Guernsey did likewise in April 2017. It is envisaged that these new laws will be in place and come into force before the end of May 2018. The precise inter-relationship between the new laws and the GDPR, for example which supervising authority will take the lead when there is a breach, has yet to be fleshed out but the goal will be for the local authority (Jersey’s Information Commissioner or Guernsey’s Data Protection Commissioner) to take the lead when Channel Island entities are involved.

Key areas of change

Penalties for non-compliance

The penalties for infringing the GDPR are much tougher than before. The revised fines
The relevant regulatory body must be notified of a data breach within 72 hours of its discovery. You may also have to notify the data subjects involved.

**Processors of data**

A “data controller” is a party that decides how and why personal data about living individuals is processed (e.g. a bank or mobile telephone company). A “data processor” acts on the data controller’s behalf (e.g. a specialist payroll company that processes staff wage payments on behalf of an employer). The GDPR will place specific legal obligations on data processors and cause them to have significantly greater liability for breaches.

In addition to continuing to abide by their numerous obligations, data controllers will have to take action to upgrade their practices in line with the GDPR regime and to also ensure that the agreements that they enter into with data processors comply with the new rules.

**Your reason for using data**

An organisation cannot control or process personal data without a legal basis for doing so. These are called “conditions for processing”. One such condition is that the individual concerned has given their consent to the data controller using their data. Under the GDPR, there are tighter rules about whether a data controller has the data subject’s “consent”. Consent must now be freely given, specific, informed and an unambiguous indication of the individual’s wishes “by a statement or by a clear affirmative action”. Many organisations that rely on consent as their legal basis for using data may not be able to say with confidence that the procedure they follow, to include the documents or devices they use to obtain consent, comply with this upgraded definition. In the words of the UK Information Commissioner’s Office: “silence, pre-ticked boxes or inactivity does not constitute consent”.

Legal bases other than consent are available to data controllers, to include where the processing by the data controller is pursuant to a contract with the individual or when the processing is pursuant to a legitimate interest of the data controller. The GDPR should prompt organisations to consider the legal basis on which they rely, and to examine alternatives to consent.

**Rights of data subjects**

Many of the existing rights in favour of data subjects are upgraded under the GDPR and new ones are added.

The right to be “informed” already exists under EU law and Jersey and Guernsey domestic law and relates to the core principle of “fair processing of information”. This extends to informing the data subject about the identity of the data controller, how the data will be processed, and the categories of data concerned. The GDPR develops this right, to include requiring data controllers to explain how long they intend to hold on to the individual’s data. This feeds into issues such as the use of privacy notices and retention policies (more on this below).

The right of “access” is another existing right which has been upgraded. Data subjects will no longer have to pay a fee to access personal data that relates to them and the data controller must respond with the information promptly and within one month of receipt (currently 40 days in Jersey and 60 days in Guernsey).

A new right afforded to individuals is the “right to erasure”, also known as the right to be forgotten. Here, data subjects can request permanent deletion of their personal data when it is no longer necessary for it to be retained by the data controller. Data controllers may refuse in specific circumstances - to include where retention of the data is necessary to comply with a legal obligation.

**Data Protection Officer (“DPO”)**

Certain organisations will be obliged to appoint a DPO. A public authority must have one. The remaining criteria are broadly drafted and include businesses that carry out large scale, systematic monitoring of individuals, or those which carry out large scale processing of special categories of data or data relating to criminal convictions and offences. The GDPR leaves open the ability of the EU and Members States to legislate for further categories where a DPO is required. Businesses may also decide to designate a DPO even if under no legal obligation to do so.
The role of a DPO is to monitor compliance with the GDPR and equivalent laws, carry out internal audits, and advise and train staff in connection with their obligations. He or she must have a prominent and independent role with the organisation and should report to the highest management level. The DPO cannot be dismissed or penalised for performing his or her duties.

The introduction of the DPO requirement is part of the increased emphasis upon accountability and good governance under the GDPR. Also encouraged are the use of data protection impact assessments (which are mandatory in certain “high risk” cases, the list of which is not closed), keeping records of processing activities, and having appropriate policies on document retention rules.

Privacy notices

A privacy notice explains, at the time of collection, what the data subject can expect to happen to his or her personal data.

The rules regarding such statements are more detailed and specific under the GDPR. The information that data controllers provide to individuals about the processing they conduct will need to be concise, transparent, intelligible and easily accessible. Plain language must be used, particularly if the data subject is a child. The information includes: the controller’s identity and contact details (e.g. the DPO); the purpose of the data processing; the legal basis for doing so; for how long the data will be kept; who will receive the data; each of the data subject’s rights; details of transfers to third countries and the safeguards that the controller has implemented; the right to complain to the relevant authority; and the right to withdraw consent if given.

Suggested course of action

For those Channel Island businesses aware of the principles, and their obligations, under the existing domestic law, the GDPR represents an evolutionary (rather than revolutionary) change, but they will still need to invest time and resources to ensure compliance post-May 2018.

See overleaf for an overview of the process that we suggest organisations follow. Our dedicated Regulatory and Compliance team can assist you with this process.
LEGAL ANALYSIS
The GDPR contains exceptions. Establish and document how the law impacts your business.

DATA AUDIT
Determine: what personal data you hold, where you hold it, where it comes from and who you share it with.

POLICY GAP ANALYSIS
Review your existing policies and procedures and identify what needs to be amended or added.

TECHNICAL GAP ANALYSIS
Review your IT systems and identify gaps in your technical capabilities.

PRIORITISATION
There may be a lot of ground to cover. Prioritise what you need to do.

IMPLEMENTATION
Implement the above, taking advice from specialists if necessary.

GDPR EFFECTIVE
For further information, please contact:

Jersey

Edward Drummond
Partner
T +44 (0)1534 814621
E edward.drummond@bedellcristin.com

David Cadin
Managing Partner
T +44 (0)1534 814701
E david.cadin@bedellcristin.com

Rebecca McNulty
Senior Associate
T +44 (0)1534 814263
E rebecca.mcnulty@bedellcristin.com

Will Austin-Vautier
Advocate | Senior Associate
T +44 (0)1534 814798
E will.austin-vautier@bedellcristin.com

Guernsey

Kate Ovenden
Managing Partner
T +44 (0)1481 812861
E kate.ovenden@bedellcristin.com

Marc Piano
Associate
T +44 (0)1481 812859
E marc.piano@bedellcristin.com

© 2017 Bedell Cristin
The information contained in this briefing is intended to provide a brief update in relation to the topics covered. The information and opinions expressed in this briefing do not purport to be definitive or comprehensive and are not intended to provide legal advice and should not be acted or relied upon as doing so. Professional advice appropriate to the specific situation should always be obtained. No responsibility or liability is accepted in connection with the content of any websites to which you may gain access from this briefing.