

DATA PROTECTION LAWS OF THE WORLD

Gibraltar



Downloaded: 20 September 2020

GIBRALTAR



Last modified 25 January 2017

LAW

A territory within the European Union (by virtue of the accession of the United Kingdom on 1 January 1973) Gibraltar implemented the EU data Protection directive 95/46 EC in 2006 with the Data Protection Act 2004 ('Act'). Enforcement is through the offices of the Data Protection Commissioner ('DPC').

DEFINITIONS

Definition of personal data

Any information relating to a Data Subject; and a Data Subject means a natural person who is the subject of Personal Data.

Definition of sensitive personal data

Information about racial or ethnic origin, religious or philosophical beliefs, trade union membership, health or sex life. The definition includes data regarding the commission or alleged commission of any offence and information on any proceedings for offences or alleged offences, the disposal of such proceedings and any sentence given.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Commissioner

Gibraltar Regulatory Authority
Suite 603 Europort
Gibraltar

T 200 74636
F 200 72166

info@gra.gi

REGISTRATION

Data controllers who process personal data must notify the Data Protection Commissioner by registering with the Gibraltar Regulatory Authority ('GRA') so that their processing of personal data may be registered and made public in the Data Protection Register, unless an exemption applies. Once registered any changes to the processing of personal data will require the Data Protection Register to be updated.

The notification must contain the following information:

- name and address of data controller and any representative
- description of the personal data being processed and the Categories to which they relate
- description of the purpose of the processing
- description of the recipients or categories of recipient to whom data will be sent
- names of any countries outside the EEA to which data is to be transferred to
- an adequate description of the security measures taken that is sufficient to allow a preliminary assessment of those measures, and
- other information reasonably required by the DPC.

DATA PROTECTION OFFICERS

There is no requirement in Gibraltar for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject has unambiguously given his consent
- the processing is necessary for the performance of a contract to which the data subject is a party, or for actions to be carried out at the request of the data subject prior to entering into a contract
- the processing is necessary in order to comply with a legal obligation to which the data controller is subject
- the processing is necessary to prevent:
 - injury or other damage to the health of the data subject
 - serious loss or damage to his property
 - to protect his vital interests where seeking consent is likely to damage those interests
- the processing is necessary for a public purpose, namely:
 - for the administration of justice
 - for the performance of a statutory function
 - for the performance of a function of Government or of a Government Minister
 - the processing is necessary for the performance of a public function carried out in the public interest, and
 - the processing is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data are supplied, except where the rights of the data subject under the European Convention of Human Rights and the Gibraltar Constitution prevail.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of more stringent conditions.

TRANSFER

Data controllers may transfer personal data out of the EEA if any of the following conditions are met:

- the country to which the data is being transferred ensures an adequate level of protection by reference to statutory parameters
- the data subject consents to the transfer
- the transfer is necessary:
 - to perform a contract between the data subject and the data controller
 - to take steps at the request of the data subject in order to enter into a contract with the data controller
 - for the agreement or performance of a contract between a third party and the data controller at the request of the data subject
 - the transfer of data is required pursuant to an international obligation of Gibraltar; – the transfer is necessary due to a substantial public interest
 - the transfer is necessary to obtain legal advice either in respect of proceedings or to establish or defend a legal right
 - the transfer is necessary to protect the vital interests of the data subject, and
 - the transfer is made as part of personal data stored on a public register.

If none of these conditions are met, data outside of the EEA may still be transferred if:

- it is to a country approved by the EU commission as safe
- it is to a US organisation falling within the Safe Harbour provisions, or
- on terms incorporating the Model Clauses or approved Corporate Binding Rules. Alternatively the data controller can apply to the DPC for specific approval on a case by case basis.

SECURITY

Data controllers must take appropriate technical and organisational measures against accidental or unlawful destruction, loss or alteration of data, or against unauthorised disclosure or access to the information, and generally against all other unlawful forms of processing.

BREACH NOTIFICATION

There is currently no mandatory requirement in the Act to report data security breaches or losses to the DPC or to data subjects. A mandatory requirement will be introduced with the transposition into Gibraltar law of the Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications) introduced by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

ENFORCEMENT

In Gibraltar, the DPC is responsible for the enforcement of the Act. If he becomes aware that the data controller is in breach of the Act, he can initiate proceedings against the data controller.

The ultimate sanction on conviction for an offence is a fine of GBP 4,000 (in the case of summary conviction in the magistrate's court) or GBP 10,000 (in the case of indictment in the Supreme Court).

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data (eg a right to 'opt out') for direct marketing purposes.

The Communications (PD&P) Regulations 2006 ('the Regulations') prohibit the use of automated calling systems without the consent of the recipient and unsolicited emails can only be sent without consent if:

- the contact details have been provided in the course of a sale or negotiations
- the marketing relates to a similar product or services, and
- the recipient was given a means of refusing the use of their contact details for marketing when they were collected.

Direct marketing emails must not disguise or conceal the identity of the sender in contravention of the E-Commerce Act. SMS marketing is also likely to be included within the prohibition on email marketing.

The restrictions on marketing by email only apply in relation to individuals and not where email marketing is sent to corporations.

ONLINE PRIVACY

The Regulations deal with the collection of location and traffic data by public electronic communications providers ('CPs') and the use of cookies (and similar technologies).

Traffic Data

Traffic Data held by a CP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- it is being used to provide a value added service, and
- consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CP for:

- the management of billing or traffic
- dealing with customer enquiries
- the prevention of fraud
- the marketing of electronic communications services, or
- the provision of a value added service.

Location Data

Location Data may only be processed for the provision of value added services with consent and where the identity of the user is anonymised. CPs are also required to take measures and put a policy in place to ensure the security of the personal data they process.

Cookie Compliance

The use and storage of cookies and similar technologies requires:

- clear and comprehensive information, and
- consent of the website user.

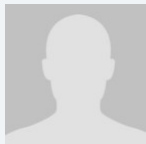
Usual data protection principals of the Act also apply. Consent is not required for cookies that are used for the sole purpose of carrying out the transmission of a communication over an electronic communications network or where this is strictly necessary for the provision of a service requested by the user.

Enforcement of a breach of the Regulations is dealt with by the DPC and if found guilty a fine and or imprisonment may be imposed. However an individual may also bring an action for damages in the Supreme Court.

KEY CONTACTS

Hassans

www.gibraltarlaw.com/



Michael Nahon

Partner

T (+350) 200 79000

michael.nahon@hassans.gi

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.