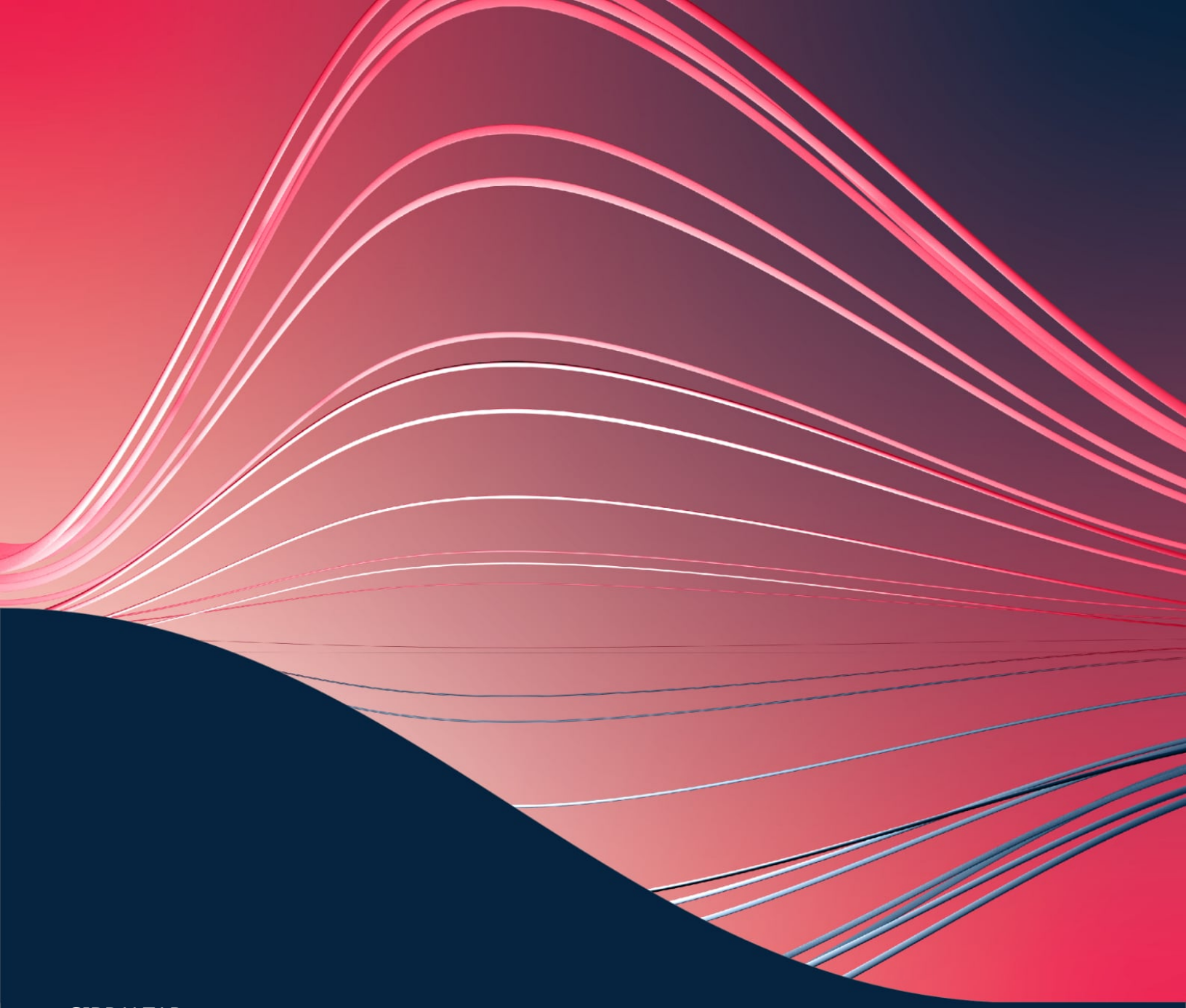


GIBRALTAR

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

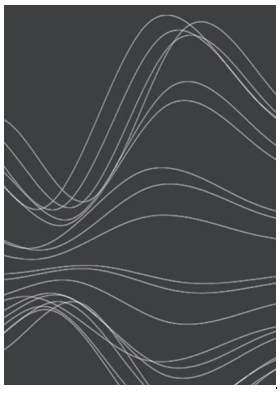
Africa key contact

Monique Jefferson
Director
monique.jefferson@dlapiper.com
Full bio

Americas key contact

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

Andrew Dyson
Partner
andrew.dyson@dlapiper.com
Full bio

Ewa Kurowska-Tober
Partner
Head of Intellectual Property and Technology, Poland
ewa.kurowska-tober@dlapiper.com
Full bio

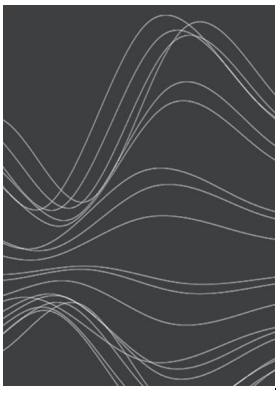
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Middle East key contact

Rami Zayat
Partner
rami.zayat@dlapiper.com
Full bio

Editors

Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



Lea Lurquin
Associate
lea.lurquin@us.dlapiper.com
Full bio

Gibraltar

LAST MODIFIED 19 JANUARY 2024

Data protection laws

Following the UK's exit from the European Union, Gibraltar ceased to be a territory within the European Union as of midnight 31st December 2020. As a consequence, the Gibraltar Government transposed the General Data Protection Regulation (Regulation (EU) 2016/679) into Gibraltar national law (thereby creating the "**Gibraltar GDPR**"). In so doing, Gibraltar made number of technical changes to the GDPR to account for its status as a national law of Gibraltar. The Gibraltar GDPR replaces EU terminology with domestic equivalents (e.g. references to "Member State law" become references to " Gibraltar law" and references to "a third country" to "a country or territory outside of Gibraltar". These changes were made under Gibraltar's Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU) Exit Regulations 2019.

All material GDPR obligations on controllers and processors remain the same under the Gibraltar GDPR.

Additionally, Gibraltar's Data Protection Act 2004 ("DPA04) remains in place as a national data protection law, and supplements the Gibraltar GDPR. It deals with matters that were previously permitted derogations and exemptions from the EU GDPR (for example substantial public interest bases for the processing of special category data, and context-specific exemptions form parts of the GDPR such as subject rights).

In addition:

- Part III of the DPA04 transposes the Law Enforcement Directive ((EU) 2016/680) into Gibraltar law, creating a data protection regime specifically for law enforcement personal data processing: and
- Parts V and VI set out the scope of the Information Commissioner's mandate and his enforcement powers, and creates a number of criminal offences relating to personal data processing.

Territorial Scope

Primarily, the application of the Gibraltar GDPR turns on whether an organization is established in GibraltarAn 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in Gibraltar.

However, the Gibraltar GDPR also has extra-territorial effect. An organization that it is not established within Gibraltar will still be subject to the Gibraltar GDPR if it processes personal data of data subjects who are in Gibraltar where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in Gibraltar or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within Gibraltar.

Definitions

Definition of personal data

"Personal data" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The Gibraltar GDPR creates more restrictive rules for the processing of "special categories" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to criminal convictions and offences (Article 10).

The Gibraltar GDPR is concerned with the "processing" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "controller" or a "processor". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the Gibraltar GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "data subject" is a living, natural person whose personal data are processed by either a controller or a processor.

"Public authority" and "public body" are expressions used in the Gibraltar GDPR. For the purposes of Gibraltar, the DPA04 defines them in S.9.

The DPA04 also clarifies that, where the purpose and means of processing are determined by an enactment of law, then the person on whom the obligation to process the data is imposed by the enactment is the controllerBottom of Form.

Definition of sensitive personal data

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 special category personal data

Information about racial or ethnic origin, religious or philosophical beliefs, trade union membership, health or sex life. The DPA04 also includes a definition on criminal convictions and offences data to include personal data relating to the 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

Gibraltar's Information Commissioner (whose functions are discharged through the Gibraltar Regulatory Authority ("**GRA**")) is the supervisory authority for Gibraltar for the purposes of Article 51 of the Gibraltar GDPR. Following Brexit the GRA will no longer be a competent supervisory authority for the purposes of the EU GDPR. The Gibraltar GDPR also omits Chapter 7 (Cooperation and Consistency) of the EU GDPR, on the basis that Gibraltar will not be part of the EU's cooperation and consistency mechanisms.

The GRA's contact details are:

Information Commissioner

Gibraltar Regulatory Authority
Suite 603 Europort
Gibraltar

T 200 74636
F 200 72166

info@gra.gi

Registration

Currently there are no registration requirements for controllers or processors under the Gibraltar GDPR.

There remains however the obligation to register Data Protection Officers with the GRA although no fee is required.

Data protection officers

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have *"expert knowledge"* (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved *"properly and in a timely manner in all issues which relate to the protection of personal data"* (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in Gibraltar GDPR, include (Article 39):

- to inform and advise on compliance with Gibraltar GDPR and other Gibraltar data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

Collection and processing

EU regulation

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");

- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the Gibraltar GDPR. Organisations must not only comply with the Gibraltar GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be *"freely given, specific, informed and unambiguous"*, and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Gibraltar law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Schedule 1 to the DPA04 supplements the requirements for processing special categories of personal data, and also provides for a number of 'substantial public interest' grounds that can be relied upon to process special categories of personal data in specific contexts which are deemed to be in the public interest. Many of these grounds are familiar from the previous UK law, whilst other are new. Important examples include:

- processing required for employment law;
- heath and social care;
- equal opportunity monitoring;
- public interest journalism;
- fraud prevention;
- preventing / detecting unlawful acts (e.g. money laundering / terrorist financing);
- insurance; and
- occupational pensions.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by domestic law (Article 10). Part 3 of Schedule 1 of the DPA authorises a controller to process criminal conviction or offences data where the processing is necessary for a purpose which meets one of the conditions in Parts 2 of Schedule 1 (this covers the conditions noted above other than processing for employment law, health and social care), as well as number of other specific conditions:

- consent;
- the protection of a data subject's vital interests; and
- the establishment, exercising or defence of legal rights, the obtaining of legal advice and the conduct of legal proceedings

Appropriate policy and additional safeguards

In any case where a controller wishes to rely on one of the DPA04 conditions to lawfully process special category, criminal conviction or offences data, the DPA04 imposes a separate requirement to have an appropriate policy document in place and apply additional safeguards to justify the processing activity. The purpose of the policy document is to set out how the controller intends to comply with each of the data protection principles in Article 5 of the Gibraltar GDPR in relation to this more sensitive processing data activity.

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data – i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The Gibraltar GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation.

Transparency (Privacy Notices)

The Gibraltar GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of Gibraltar GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, replicating those in the EU GDPR. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "which produces legal effects concerning [the data subject]… or similarly significantly affects him or her" is only permitted where:

- necessary for entering into or performing a contract;
- authorised by Gibraltar law; or
- the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Child's consent to information society services (Article 8)

Article 8(1) of the Gibraltar GDPR stipulates that a child may only provide their own consent to processing in respect of information society (primarily, online) services, where that child is over 16 years of age, unless Gibraltar applies a lower age. The DPA04 reduces the age of consent for these purposes to 13 years for Gibraltar.

Gibraltar regulation

Automated Decision Making (Article 22)

Automated decision making (including profiling) "which produces legal effects concerning [the data subject]… or similarly significantly affects him or her" is only permitted where:

- necessary for entering into or performing a contract;
- authorised by Gibraltar law; or
- the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view. Further safeguards for automated decisions that are necessary for entering into or performing a contract or which are authorised by Gibraltar law are set out in section 17 of the DPA04.

Transfer

Transfers from Gibraltar

Transfers of personal data by a controller or a processor to third countries outside of Gibraltar are only permitted where the conditions laid down in Chapter V of the Gibraltar GDPR are met (Article 44).

Article45(1) allows transfers of personal data to:

- third countries on the basis of UK adequacy regulations made under UK GDPR and Part 2 of the UK Data Protection Act 2018; and
- to the United Kingdom.

Currently, the following countries or territories enjoy UK adequacy decisions (these have all essentially been 'rolled over', on a temporary basis, from the EU GDPR with some additions): Andorra, Argentina, Canada and Japan (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay, South Korea and New Zealand. Also included are transfers to the USA, if covered under the UK extension to the EU-US Data Privacy Framework.

The UK is also currently treating all EU and EEA Member States as adequate jurisdictions. Therefore transfers to any of the above jurisdictions from Gibraltar will not require any additional safeguards Gibraltar GDPR.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available (Article 46). The list of appropriate safeguards includes, amongst others, binding corporate rules and the use of standard contractual clauses with additional safeguards to guarantee an essentially equivalent level of protection to data subject's and their personal data.

Section 128A of the DPA04 allows Gibraltar's Information Commissioner to publish standard data protection clauses which comply with Article 46 requirements. To date, a bespoke International Data Transfer Agreement ("**IDTA**") has been published for data exports from Gibraltar in addition to an International Data Transfer Addendum ("**Addendum**"). Both the IDTA and Addendum can be used. Whereas the IDTA is a full-form standalone agreement, the Addendum is to be used along-side the EU Standard Contractual Clauses for use in the context of the Gibraltar GDPR.

Article 49 of the UK GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

- explicit informed consent has been obtained;
- the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between
- the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
- the transfer is made from a register which according to domestic law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to Gibraltar's Information Commissioner and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside Gibraltar t(Article 48) are only recognised or enforceable (within Gibraltar) where they are based on an international agreement which applies to Gibraltar such

as a mutual legal assistance treaty in force between the requesting third country and Gibraltar ; a transfer in response to such requests where there is no other legal basis for transfer will infringe the Gibraltar GDPR.

Transfers from the UK to Gibraltar

Gibraltar and the UK enjoy the free flow of personal data without the need for any additional safeguards.

ibraltar is now a third country for the purposes of Chapter V of the EU GDPR. Unlike the UK, Gibraltar does not currently benefit from an EU adequacy decision. It is expected that Gibraltar will obtain EU adequacy with the conclusion of the UK-EU treaty on Gibraltar. Until then, alternative EU GDPR Chapter V safeguards are required to transfer personal data from the EU to Gibraltar.

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the Gibraltar GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the Gibraltar GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Breach notification

The Gibraltar GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

Mandatory breach notification

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in

a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Personal data breaches should be notified to GRA as Gibraltar's supervisory authority. Breaches must be reported to the GRA using their Data Breach Notification Form available on their website and sent by email to dpbreach@gra.gi.

Enforcement

Fines

The Gibraltar GDPR empowers the Information Commissioner to impose fines of up to 4% of annual worldwide turnover, or £17.5 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to £17.5 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;

- obligations of certification bodies; and
- obligations of a monitoring body.

The Information Commissioner is not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

The information Commissioner also enjoys a wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The Gibraltar GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the Gibraltar GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with the Information Commissioner (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The DPA04 sets out the specific enforcement powers provided to the GRA pursuant to Article 58 of the GDPR, including:

- information notices – requiring the controller or processor to provide the GRA with information;
- assessment notices – permitting the GRA to carry out an assessment of compliance;
- enforcement notices – requiring the controller or processor to take, or refrain from taking, certain steps; and
- penalty notices – administrative fines.

The Information Commissioner has the power to conduct a consensual audit of a controller or a processor, to assess whether that organisation is complying with good practice in respect of its processing of personal data.

Under Schedule 15 of the DPA04 the Information Commissioner also has powers of entry and inspection. These will be exercised pursuant to judicial warrant and will allow the Information Commissioner to enter premises and seize materials.

The DPA04 creates two new criminal offences in Gibraltar law: the re-identification of de-identified personal data without the consent of the controller and the alteration of personal data to prevent disclosure following a subject access request under Article 15 of the GDPR. The DPA04 retains existing Gibraltar criminal law offences, e.g. offence of unlawfully obtaining personal data.

The DPA04 requires the Information Commissioner to issue guidance on its approach to enforcement, including guidance about the circumstances in which it would consider it appropriate to issue a penalty notice, i.e. administrative fine.

The DPA04 also allows the Information Commissioner to publish statutory codes of practice on direct marketing and data sharing.

Electronic marketing

The Gibraltar GDPR applies to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing is consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the Gibraltar GDPR are to be noted, and marketing consent forms invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local law under the Communications (Personal Data and Privacy) Regulations 2006 (the Regulations). EU Member States are supposed to replace the ePrivacy Directive with a Regulation. However, there is still no certainty when this is going to happen. Should this happen, Gibraltar will likely need to adopt any such legislation into its own domestic law.

In the meantime, Gibraltar GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the Gibraltar GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive have been replaced with the Gibraltar GDPR standard for consent.

The Regulations apply to most electronic marketing activities. The Regulations do not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to 'opt-out' for direct marketing purposes.

There are a number of different opt-out schemes / preference registers for different media types. Individuals (and, in some cases, corporate subscribers) can contact these schemes and ask to be registered as not wishing to receive direct marketing material. If advertising materials are sent to a person on the list, sanctions can be levied by the Information Commissioner.

The Regulations also prohibit the use of automated calling systems without the consent of the recipient and the use of unsolicited electronic communications (i.e. by email or SMS text) for direct marketing purposes is also prohibited without prior consent from the consumer unless:

- the consumer has provided their relevant contact details in the course of purchasing a product or service from the person proposing to undertake the marketing;
- the marketing relates to offering a similar product or service; and
- the consumer was given a means to readily 'opt out' of use for direct marketing purposes both at the original point where their details were collected and in each subsequent marketing communication.

Each direct marketing communication must not disguise or conceal the identity of the sender and include the 'unsubscribe' feature referred to above.

The restrictions on marketing by email / SMS only applies in relation to individuals and not where marketing to corporate subscribers.

Online privacy

The Communications (Personal Data and Privacy) Regulations 2006 (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.

The GRA's position is positive action e.g. via the use of tick box will be required by the user for the installation of cookies and that pre enabled boxes do not amount to consent. Usual data protection principals of the Gibraltar GDPR also apply.

Note 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.

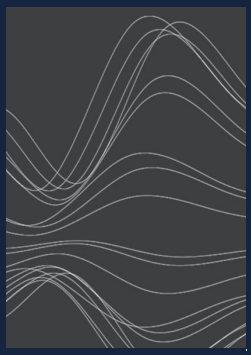
Enforcement of a breach of the Regulations is dealt with by the Information Commissioner and if found guilty a fine and or imprisonment may be imposed. However an individual may also bring an action for damages in the Supreme Court.

Data protection lawyers

Michael Nahon
Partner
Hassans
michael.nahon@hassans.gi
View bio

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com