

DATA PROTECTION LAWS OF THE WORLD

South Africa vs United Kingdom



Downloaded: 26 April 2024

SOUTH AFRICA



Last modified 17 January 2024

LAW

The right to privacy is recognized as a fundamental human right in the Bill of Rights of the Constitution of the Republic of South Africa and is protected in terms of the Constitution and the common law. This right to privacy is not absolute and may be limited where it is reasonable and justifiable to do so.

The Protection of Personal Information Act 4 of 2013 (POPIA) came into effect on 1 July 2020 but was subject to a one year grace period which ended on 30 June 2021. POPIA specifically regulates the processing of personal information that is entered into a record pertaining to natural living persons as well as existing legal persons.

UNITED KINGDOM



Last modified 22 January 2024

LAW

Following the UK's exit from the European Union, the UK Government has transposed the General Data Protection Regulation (Regulation (EU) 2016/679) into UK national law (thereby creating the **UK GDPR**). In so doing, the UK has made a number of technical changes to the GDPR in order account for its status as a national law of the United Kingdom (e.g. to change references to **Member State**; to **the United Kingdom**). These changes were made under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. *At this time, all material obligations on controller and processors essentially remain the same under the UK GDPR as under the EU GDPR.*

The Data Protection Act 2018 (**DPA**) remains in place as a national data protection law, and supplements the UK GDPR regime. 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 from parts of the GDPR such as data subject rights).

In addition,

- Part 3 of the DPA transposes the Law Enforcement Directive ((EU) 2016/680) into UK law, creating a data protection regime specifically for law enforcement personal data processing;
- Part 4 of the DPA updates the data protection regime for national security processing; and
- Parts 5 and 6 set out the scope of the Information Commissioner's mandate and her enforcement powers, and creates a number of criminal offences relating to personal data processing.

On 8 March 2023, the new **Data Protection and Digital Information (No. 2) Bill**; (**the Bill**) was introduced to Parliament following on

from the consultation by the Department for Culture, Media and Sport on data protection reforms. The anticipated reforms aim to reduce the compliance burden on organisations. A few of the proposed changes in the Bill include:

- Amendments to certain definitions, such as 'identifiable living individual' (impacting the definition of 'personal data') and the meaning of research and statistical purposes;
- Amendments to data protection principles, including the addition of recognised 'legitimate interests' to assist with determining an applicable legal basis;
- Amendments to the conduct of data subject rights, by recognising requests that may be 'vexatious or excessive'; and
- Amendments to the obligations of controllers and processors which generally provide more flexibility than the current position, for example with regard to complying with accountability obligations.

It is expected that the Bill will be debated and amended further as it passes through the House of Lords in the first months of 2024, and will likely be enacted through the course of the year.

Territorial Scope

The application of the UK GDPR turns principally on whether an organization is established in the United Kingdom. As under the EU GDPR, an 'establishment' may take a wide variety of forms, and is not limited to a company registered in the United Kingdom.

The UK GDPR also has extra-territorial effect, following the same principles as set out in the EU GDPR. As a result, an organisation that it is not established within the United Kingdom will be subject to the UK GDPR if it processes personal data of data subjects who are in the United Kingdom where the processing activities are related "to the offering of goods or services" (Article 3(2)(a)) to such data subjects in the United Kingdom or "the monitoring of their behaviour" (Article 3(2)(b)) as far as their behaviour takes place within the United Kingdom.

DEFINITIONS

Definition of personal data

"Personal information" is defined in POPIA as information relating to an identifiable, living, natural person, and

DEFINITIONS

"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

where applicable, an identifiable, existing, juristic person, including:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin; color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief; culture, language and birth of the person;
- Information relating to the education, medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- The biometric information of the person;
- The personal opinions, views or preferences of the person;
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- The views or opinions of another individual about the person; and
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

POPIA applies to the processing of personal information entered in a record by or for a responsible party / data controller that is domiciled in South Africa and that makes use of automated or non-automated means to process the personal information. It would also apply if the responsible party is not domiciled in South Africa but makes use of automated or non-automated means in South Africa unless those means are used only to forward personal information through South Africa.

POPIA does not apply to the processing of personal information:

- In the course of a purely personal or household activity;
- That has been de-identified to the extent that it cannot be re-identified again;
- By or on behalf of the State with regard to national security, defense or public safety, or the prevention, investigation or proof of offenses; or for the purposes of the prosecution of offenders or the execution of sentences or security

person can be identified using any 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 UK 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 UK 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 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 UK GDPR. The DPA defines them by reference to the definition of "public authority" used in the Freedom of Information Act 2000.

The DPA 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 controller.

measures, to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information;

- For exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information;
- Solely for the purposes of journalistic, literary or artistic expression to the extent that such exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression;
- By Cabinet and its committees, the Executive Council of a province and a Municipal Council of a municipality;
- For purposes relating to the judicial functions of a court referred to in section 166 of the Constitution; and
- Under circumstances that have been exempted from the application of the conditions for lawful processing by the Information Regulator in certain circumstances.

Definition of sensitive personal data

Special personal information is information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information and criminal behavior (to the extent that such information relates to the alleged commission of an offense or any proceedings in respect of any offence allegedly committed, or the disposal of such proceedings).

Subject to certain prescribed exceptions, the processing of special personal information without the consent of the data subject is generally prohibited under POPIA.

NATIONAL DATA PROTECTION AUTHORITY

The Information Regulator has established an Enforcement Committee and initiates investigations into various possible violations of POPIA. There is scrutiny by the Information Regulator into security compromises including the establishment of a security compromise register. These activities are in line with the powers, duties and functions of the office of the Information Regulator which include providing education regarding the protection and processing of personal information; monitoring and enforcing compliance with the provisions

NATIONAL DATA PROTECTION AUTHORITY

The Information Commissioner (whose functions are discharged through the Information Commissioner's Office ("**ICO**")) is the supervisory authority for the UK for the purposes of Article 51 of the UK GDPR. Following Brexit, the ICO no longer has influence or membership in the European Data Protection Board and can no longer be nominated as a lead supervisory authority under the EU GDPR regime. This is reflected in the UK GDPR which omits Chapter 7 (Cooperation and Consistency) of the EU GDPR, on the basis that the UK

of POPIA; consulting with interested parties and acting as mediator; receiving, investigating and attempting to resolve complaints; issuing enforcement notices and codes of conduct; and facilitating cross-border cooperation.

REGISTRATION

Data protection officers (referred to in POPIA as "**information officers**") must be registered with the Information Regulator.

Responsible parties are required to obtain prior authorization from the Information Regulator before processing personal information in certain circumstances prescribed in section 57 of POPIA, for example, where special personal information or personal information of children is transferred to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information and where information on criminal behavior or unlawful or objectionable conduct is processed on behalf of third parties. Prior authorization is also required when processing personal information for the purposes of credit reporting or when processing unique identifiers for a purpose other than the purpose for which it was originally collected and linking it with personal information processed by other third parties. Responsible parties are not otherwise required to register their processing of personal information.

The prior authorization requirements in POPIA came into effect on 1 February 2022. This means that all responsible parties (i.e. data controllers) that conduct processing activities that are subject to prior authorization need to submit an application for prior authorization and will need to cease such processing activities until such time as prior authorization is obtained.

DATA PROTECTION OFFICERS

will not be part of the EU's cooperation and consistency mechanisms.

The ICO's contact details are:

Wyldiffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

T +0303 123 1113 (or +44 1625 545745 if calling from overseas)

F 01625 524510

www.ico.org.uk

REGISTRATION

The UK operates a fee-paying scheme for controllers under the Data Protection (Charges and Information) Regulations 2018, known as the "Data Protection Fee". All controllers have to pay the data protection fee to the ICO annually, unless they are exempt from doing so.

The UK Government has set the fee tiers based on its perception of the risks posed by controllers processing personal data. The amount payable depends upon staff numbers and annual turnover or whether the controller is a public authority, a charity or a small occupational pension scheme. Not every controller must pay a fee; there are exemptions. The maximum fee, for large organisations, is GBP 2,900.

The maximum penalty for a controller who breaks the law by not paying a fee (or not paying the correct fee) is a fine of GBP 4,350 (150% of the top tier fee).

DATA PROTECTION OFFICERS

Data protection officers (referred to in POPIA as "**information officers**") must be registered with the Information Regulator. The duties and responsibilities of a responsible party's information officer are set forth in POPIA and include encouraging and ensuring compliance with POPIA; dealing with any requests made to that responsible party in terms of POPIA; and working with the Information Regulator in respect of investigations by the Information Regulator in relation to that responsible party. The Regulations to POPIA, among other things, further provide that the information officer must ensure that a compliance framework is developed, implemented, monitored and maintained, and that a personal information impact assessment is conducted to ensure that adequate measures and standards for the protection of personal information exist.

COLLECTION & PROCESSING

"Processing" of information is defined in POPIA as any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

Under the UK GDPR, 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 the UK GDPR, include (Article 39):

- to inform and advise on compliance with the UK GDPR and other UK 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 & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal

- The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- Dissemination by means of transmission, distribution or making available in any other form; and
- Merging, linking, as well as blocking, degradation, erasure or destruction of information.

POPIA prescribes the following eight conditions for lawful processing of personal information:

- **Accountability:** The responsible party must comply with all the conditions for lawful processing.
- **Purpose specification:** Personal information must only be collected for a specific, explicitly defined lawful purpose related to a function or activity of the responsible party.
- **Processing limitation:** Processing must be justified on a ground recognized under POPIA (e.g. consent / legitimate interests of the data subject, responsible party or the third party to whom the information is supplied).
- **Further processing limitation:** Processing must be in accordance with or compatible with the purpose for which it was initially collected subject to limited exceptions.
- **Information quality:** Steps must be taken to ensure that the information is complete, accurate, not misleading and updated where necessary.
- **Openness:** Notification requirements must be complied with when collecting personal information.
- **Security safeguards:** Appropriate, reasonable technical and organizational measures must be implemented and maintained to prevent loss of, damage to or unauthorized destruction of or unlawful access to personal information.
- **Data subject participation:** Data subjects have the right to request details of the personal information that a responsible party holds about them and, in certain circumstances, request access to such information.

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 UK GDPR. Organisations must not only comply with the UK 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 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 (under UK law) 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 Categories of Personal Data

Processing of special categories of personal 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 United Kingdom 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 DPA 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;
- health and social care;
- equal opportunity monitoring;
- public interest journalism;
- fraud prevention;
- preventing / detecting unlawful acts (eg money laundering / terrorist financing);
- insurance; and
- occupational pensions.

Criminal convictions and offences data (Article 10)

The processing of criminal conviction or offences data is prohibited by Article 10 of the UK GDPR, except where specifically authorised under relevant member state law. 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 DPA conditions to lawfully process special category,

criminal conviction or offences data, the DPA 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 UK 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 UK 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 UK 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 UK 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.

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 .xml).

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 UK 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 UK law are set out in section 14 of the DPA.

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

Article 8(1) of the UK 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 UK law applies a lower age. The DPA reduces the age of consent for these purposes to 13 years for the UK.

TRANSFER

POPIA caters for two scenarios relating to the transfer of personal information, namely where a responsible party in South Africa sends personal information to another country to be processed and where a responsible party in South Africa processes personal information that has been received from outside South Africa.

Receiving personal information from other countries

The requirements for the processing of personal information prescribed in POPIA will apply to any personal information processed in South Africa, irrespective of its origin.

TRANSFER

Transfers from the UK

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

The United Kingdom Government has the power to make an adequacy decision in respect of a third country under the UK GDPR (Article 45). This power is equivalent to the similar authorities granted to the EC has under the EU GDPR and involves the Secretary of State making a positive determination that the third country provides for adequate level of data protection, following

Sending personal information to other countries for processing

A responsible party in South Africa may not transfer personal information to a third party in another country unless:

- The recipient is subject to a law, binding corporate rules or a binding agreement which:
 - Upholds principles for reasonable processing of the information that are substantially similar to the conditions contained in POPIA; and
 - Includes provisions that are substantially similar to those contained in POPIA relating to the further transfer of personal information from the recipient to third parties who are in another country;
- The data subject consents to the transfer;
- The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; or
- The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; or
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party, or the transfer is for the benefit of the data subject and:
 - It is not reasonably practicable to obtain the consent of the data subject to that transfer; and
 - If it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

which personal data may be freely transferred to that third country (Article 45(1)). On 21 September 2023, the United Kingdom Government adopted its adequacy decision for the UK Extension for the EU-US Data Privacy Framework, in which an adequate level of protection for personal data transferred the UK to US companies that have joined the framework is ensured in accordance with UK GDPR Art. 45. 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): Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Eastern Republic of Uruguay, United States (if certified under the UK Extension to the EU-US Data Privacy Framework) and New Zealand. The UK is also treating all EU and EEA Member States as adequate jurisdictions, again on a temporary basis. The United Kingdom intends to reassess all these adequacy decisions before the end of 2024. It also has the power to make its own adequacy decisions, and likely time consider new candidates for UK adequacy.

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 standard contractual clauses with additional safeguards to guarantee an essentially equivalent level of protection to data subject's and their personal data¹.

Schedule 21 to the DPA provides that the EU Commission approved standard contractual clauses may continue to be used for transfers under the UK GDPR, until such time as they replaced by clauses issued by the UK Government. Note that the standard contractual clauses carried into UK law are those which were in use as at the end of 2020. It is expected these will be updated during the course of 2021.

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 the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the United Kingdom (Article 48) are only recognised or enforceable (within the United Kingdom) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the United Kingdom; a transfer in response to such requests where there is no other legal basis for transfer will infringe the UK GDPR.

Transfers from the EU to the UK

The UK is now a third country for the purposes of Chapter V of the EU GDPR .

On 28 June 2021, the EU adopted adequacy decisions in relation to the UK, recognising that the UK offers an equivalent level of protection of personal data as compared to the EU. This therefore enables personal data to flow freely from the EU to the UK.

For more information, please visit our [Transfer - global data transfer methodology website](#).

SECURITY

Section 19 of POPIA places an obligation on a responsible party to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss, damage to, or unauthorised destruction of, and unlawful access to, personal information.

To comply with this obligation, the responsible party must take reasonable measures to do all of the following:

- Identify all reasonably foreseeable internal and external risks to personal information under its control;
- Establish and maintain appropriate safeguards against the risks identified;
- Regularly verify that the safeguards are effectively implemented; and
- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

The responsible party must also have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

BREACH NOTIFICATION

In terms of section 22 of POPIA, where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Information Regulator and the data subject, unless the identity of such data subject cannot be established.

The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or

I. Following the decision of the Court of Justice of the European Union in the *Data Protection Commissioner v. Facebook and Max Schrems* case (the *Schrems II* case)

SECURITY

The UK GDPR is not prescriptive about specific technical standards or measures. Rather, the UK 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 UK GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- 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
- 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 UK GDPR contains a general requirement for a personal data breach to be notified by the controller to the ICO, 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).

The controller must notify a breach to the ICO 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

any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offenses or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned and must be in writing and communicated to the data subject in a prescribed manner.

The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including all of the following:

- A description of the possible consequences of the security compromise;
- A description of the measures that the responsible party intends to take or has taken to address the security compromise;
- A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- If known to the responsible party, the identity of the unauthorized person who may have accessed or acquired the personal information.

The Information Regulator may direct a responsible party to publicize, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Information Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

An operator / data processor is not required to notify the Information Regulator or data subjects where there are reasonable grounds to believe that there has been a data breach. It must, however, notify the responsible party / data controller of the suspected data breach.

ENFORCEMENT

Any person may submit a complaint to the Information Regulator alleging non-compliance with POPIA. The Information Regulator may also initiate an investigation into interference with the protection of personal information.

Upon receipt of a complaint, the Information Regulator may, inter alia, conduct a pre-investigation or full

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 ICO 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 ICO.

Breaches in the United Kingdom can be reported to the ICO's dedicated breach helpline during office hours (+44 303 123 1113). Outside of these hours (or where a written notification is preferred) a pro forma may be downloaded and emailed to the ICO.

ENFORCEMENT

Fines

The UK GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or GBP 17.5 million (whichever is higher).

It is the intention that fines should, where appropriate, be imposed by reference to the revenue of an economic

investigation of the complaint, act as conciliator, refer the complaint to another regulatory body if the Information Regulator considers that the complaint falls more properly within the jurisdiction of the other regulatory body, or decide to take no further action.

The Information Regulator's powers, for purposes of investigating a complaint include the power to summons and enforce the appearance of persons before the Information Regulator to give evidence or produce records or things; enter and search the premises occupied by a responsible party; and conduct interviews and inquiries.

If the Information Regulator is satisfied that a responsible party has interfered or is interfering with the protection of the personal information of a data subject it may issue an enforcement notice prescribing action to be taken by the responsible party to remedy the situation.

A responsible party who fails to comply with an enforcement notice is guilty of an offense and is, liable, on conviction, to a fine or imprisonment (or both) for a period of no longer than ten years (in terms of section 107), or alternatively to an administrative fine (in terms of section 109). Currently, the maximum fine under sections 107 and 109 of POPIA is R10 million.

Section 99 also makes provision for a civil action for damages resulting from non-compliance with POPIA. In order to succeed in such a claim the complainant would need to prove all the elements of a delict: wrongful conduct, causation, fault (intent / negligence) and harm. The data subject would need to prove the quantum of the damages that s/he seeks.

undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the UK GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to GBP 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 domestic 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 GBP 8.7 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 ICO 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. To date, the ICO has issued several fines under GDPR, ranging from GBP 275,000 to GBP 20 million.

Investigative and corrective powers

The ICO also enjoys 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 UK 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 UK 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 ICO (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of the ICO 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 DPA sets out the specific enforcement powers provided to the ICO pursuant to Article 58 of the UK GDPR, including:

- information notices § 58(1); requiring the controller or processor to provide the ICO with information;
- assessment notices § 58(1); permitting the ICO to carry out an assessment of compliance;
- enforcement notices § 58(1); requiring the controller or processor to take, or refrain from taking, certain steps; and
- penalty notices § 58(1); administrative fines.

The ICO 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 DPA, the ICO also has powers of entry and inspection. These will be exercised pursuant to judicial warrant and will allow the ICO to enter premises and seize materials.

The DPA creates two new criminal offences in UK 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 DPA retains existing UK criminal law offences, eg offence of unlawfully obtaining personal data.

The DPA requires the ICO 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 DPA also requires the ICO to publish statutory codes of practice on direct marketing and data sharing (preserving the position under the previous law).

ELECTRONIC MARKETING

Direct marketing by means of unsolicited electronic communications is regulated by POPIA whereby the opt-in regime has taken effect. Accordingly, under POPIA, the processing of a data subject's personal information for the purposes of direct marketing by means of unsolicited electronic communications is prohibited unless the data subject has given its consent, or the email recipient is an existing customer of the responsible party. A responsible party may only approach a data subject once in order for the data subject to opt in to receive marketing information. The Regulations to POPIA contain a prescribed form to be used when seeking this opt-in.

When sending emails to a data subject who is an existing customer:

- a. the responsible party must have obtained the details of the data subject through a sale of a product or service;
- b. the marketing should relate to its own similar products or services; and
- c. the data subject must have been given a reasonable opportunity to opt out, free of charge, of the use of its personal information for marketing when such information was collected and on each occasion that marketing information is sent to the data subject, if the data subject has not initially refused the use of the personal information for electronic marketing purposes.

Direct marketing that is not by electronic communications (i.e. telephone or in-person marketing) continues to be regulated by the Consumer Protection Act, which requires the consumer to have an opportunity to opt out of receiving direct marketing.

ELECTRONIC MARKETING

The UK GDPR will apply 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 will be 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 UK GDPR are to be noted, and marketing consent forms will 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 found in the Privacy and Electronic Communications Regulations 2003 (as amended) (**PECR Regulations**). The PEC Regulations are derived from European Union Directive 2002/58/EC (ePrivacy Directive), which have been retained in UK law post-Brexit.

The PEC Regulations prohibit the use of automated calling systems without the consent of the recipient. The PEC Regulations also prohibit unsolicited electronic communications (ie by email or SMS text) for direct marketing purposes 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.

Enforcement of a breach of the PEC Regulations is dealt with by the ICO. The maximum fine for a breach of the PEC Regulations is GBP 500,000, which can be issued against a company or its directors. The ICO regularly issues fines for direct marketing violations, and it is not uncommon for these to be in the hundreds of thousands of pounds range.

ONLINE PRIVACY

There are no sections of POPIA that expressly regulate privacy in relation to cookies and location data. These issues may be dealt with in subsequent regulations or codes of conduct to be issued by the Information Regulator.

ONLINE PRIVACY

The PEC Regulations (as amended) deal with the collection of location and traffic data by public electronic communications services providers ("**CSPs**") and use of cookies (and similar technologies).

Traffic Data

Traffic Data held by a CSP 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 also be processed by a CSP to the extent necessary for:

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

Cookie Compliance

The use and storage of cookies and similar technologies requires:

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

The ICO released comprehensive guidance on the use of cookies and similar technologies in 2019. In line with the standard for ‘GDPR like’ consent under the PEC Regulations, this guidance significantly raised the bar in terms of the ICO’s expectations for cookie consent collection. It is now clear that the ICO expects consent to be collected on a clear opt-in basis; implied consent (such as the continued browsing of a website after being shown a cookie banner) is no longer sufficient. Instead, cookie consent modules that given users granular choices about cookie selection (typically on a ‘by purpose’ basis) are becoming the norm in order to align with the guidance.

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
- strictly necessary for the provision of a service requested by the user.

Enforcement of a breach of the PEC Regulations is dealt with by the ICO. The maximum fine for a breach of the PEC Regulations is GBP 500,000, which can be issued against a company or its directors.

KEY CONTACTS

DLA Piper



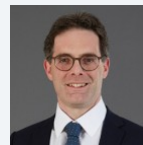
Monique Jefferson
Director
T +27 11 302 0853
monique.jefferson@dlapiper.com



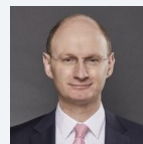
Justine Katz
Associate
T +27 (0) 11 302 0846
justine.katz@dlapiper.com

DATA PRIVACY TOOL

KEY CONTACTS



Andrew Dyson
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +44 (0) 113 369 2403
andrew.dyson@dlapiper.com



Ross McKean
Partner
T +44 (0) 20 7796 6077
ross.mckean@dlapiper.com



James Clark
Partner
T +44 113 369 2461
james.clark@dlapiper.com

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

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 © 2022 DLA Piper. All rights reserved.