Comparing privacy laws:
GDPR v. Data Protection Regulations 2021

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Image production credits:
Cover/p.5/p.51: 221A / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents

Introduction 5

1. Scope
1.1. Personal scope 7
1.2. Territorial scope 9
1.3. Material scope 11

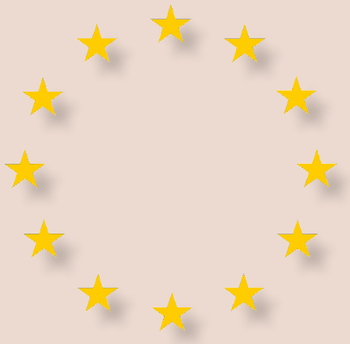
2. Key definitions
2.1. Personal data 13
2.2. Pseudonymisation 15
2.3. Controller and processors 16
2.4. Children 18
2.5. Research 19

3. Legal basis 22

4. Controller and processor obligations
4.1. Data transfers 24
4.2. Data processing records 26
4.3. Data protection impact assessment 29
4.4. Data protection officer appointment 33
4.5. Data security and data breaches 35
4.6. Accountability 37

5. Individuals' rights
5.1. Right to erasure 38
5.2. Right to be informed 42
5.3. Right to object 45
5.4. Right of access 48
5.5. Right not to be subject to discrimination 50
5.6. Right to data portability 51

6. Enforcement
6.1. Monetary penalties 53
6.2. Supervisory authority 56
6.3. Civil remedies for individuals 61



Introduction

The Abu Dhabi Global Market ('ADGM') is a Financial Free Zone within the UAE, which itself is a Federation composed of seven Emirates. Being a Financial Free Zone, UAE federal civil and commercial law does not apply, and the ADGM is able to create its own legal and regulatory framework for all civil and commercial matters.

In the ADGM, the Board of Directors of the ADGM enacted, on 11 February 2021, the Data Protection Regulations 2021 ('the Regulations') which make provision for the protection of personal data processed or controlled from within the ADGM, and thus govern the processing of personal data by persons operating in the Free Zone. In particular, the Regulations provide for a 12-month transition period for current establishments, as well as for a six months transition period for new establishments, being enforceable from 14 August 2021 and 14 February 2022. The Data Protection Regulations 2015, as amended by Data Protection (Amendment) Regulations 2018 ('Data Protection Regulations 2015') remained applicable until these dates.

The aim of the Regulations is to bring the ADGM data protection regime in line with international standards such as the EU's General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR').

The newly established Office of Data Protection is the Regulations' independent supervisor, headed by the Commissioner of the Office of Data Protection, as appointed by the Board of Directors of the ADGM.

The Office of the Data Protection have spotlighted, for example in their Overview of the 2021 Regulations for New Entities, that the Regulations are closely aligned with the UK GDPR/EU GDPR, as is evident throughout this report.

Following the conclusion of the transition period for new establishments, the ADGM updated their guidance to be in line with the 2021 Regulations, which include the following:

- Guidance on the Data Protection Regulations Part 1: Overview of Regulations and key concepts, terms, scope, principles of processing, and the lawful bases for processing personal data
- Guidance on the Data Protection Regulations Part 2: Data subject rights
- Guidance on the Data Protection Regulations 2021 Part 3: Addressing data protection by design and default, fees, the record of processing activities ('ROPAs'), the requirement for a data protection officer ('DPO') and processor obligations
- Guidance on the Data Protection Regulations 2021 Part 4: Data Protection Impact Assessments
- Guidance on the Data Protection Regulations 2021 Part 5: Security of processing, cessation of processing, personal data breach notifications
- Guidance on the Data Protection Regulations 2021 Part 6: International Transfers
- Guidance on the Data Protection Regulations 2021 Part 7: Codes of conduct and role of Office/Commissioner of Data Protection
- Guidance on the Data Protection Regulations 2021 Part 8: Individuals' Rights and Remedies

Differences between the Regulations and their predecessor, the Data Protection Regulations 2015, include new accountability requirements, the appointment of a Data Protection Officer ('DPO'), carrying out Data Protection Impact Assessments ('DPIAs'), data processing agreements with vendors, data breach notifications, and monetary penalties enforceable by the new authority, among many other things.

Structure and overview of the Guide

This Guide provides a comparison of the two legislative frameworks on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant provisions from the two legislative legal frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the Regulations.

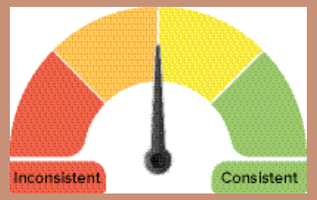
Key for giving the consistency rate

Consistent: The GDPR and the Regulations bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and the Regulations bear a high degree of similarity in the rationale, core, and the scope of the provision considered, however, the details governing its application differ.

Fairly inconsistent: The GDPR and the Regulations bear several differences with regard to the scope and application of the provision considered, however, its rationale and core presents some similarities.

Inconsistent: The GDPR and the Regulations bear a high degree of difference with regard to the rationale, core, scope, and application of the provision considered.



Usage of the Guide

This Guide is general and informational in nature, and is not intended to provide, and should not be relied on as a source of, legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be Regulationsed upon without specific legal advice based on particular circumstances.

1. Scope

1.1. Personal scope

The GDPR and the Regulations adopt consistent core definitions, including the concepts of controller, processor, data subject, and public bodies. The Regulations do not make a reference to deceased individuals, but at the same time defines data subjects as living natural persons, adopting a consistent approach with the GDPR, which does not apply to deceased individuals. Lastly, both the GDPR and the Regulations apply to natural persons whatever their nationality or place of residence.

GDPR	Regulations
Data controller	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Section 62(1): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Section 62(1): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data subject	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fRegulationsors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 62(1): 'data subject' means an identified or identifiable living natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Public bodies	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Section 62(1): 'controller' means the natural or legal person, public authority, agency or other body [...].

GDPR	Regulations
Nationality of data subject	
Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.	Section 3(3): The Regulations apply to natural persons whatever their nationality or place of residence.
Place of residence	
See Recital 14, above.	See Section 3(3) above.
Deceased individuals	
Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.	The Regulations do not refer to deceased individuals. However, Section 62(1) defines a 'data subject' as an identified or identifiable living natural person.

1.2. Territorial scope

Fairly consistent

Both the GDPR and the Regulations apply extraterritorially to the activities of controllers or processors in the territory, irrespective of location of the processing activity, as well as the nationality or residence of the individual. The Regulations do clarify that an 'establishment' pertains to any authority, body corporate, branch, representative office, institution entity, or project established, registered or licensed to operate or conduct any activity within the ADGM or exempt from being registered or licensed under the laws of the ADGM.

GDPR	Regulations
Establishment in jurisdiction	
Article 3: This Regulation applies to the processing of personal data in the context of the Regulationsivities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Recital 22: Establishment implies the effective and real exercise of Regulationsivity through stable arrangements.	Section 3(1): The Regulations apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in ADGM, regardless of whether the processing takes place in ADGM or not. Section 62(1): 'establishment' means any authority, body corporate, branch, representative office, institution entity, or project established, registered or licensed to operate or conduct any activity within the ADGM or exempt from being registered or licensed under the laws of the ADGM.
Extraterritorial	
See Article 3, above.	See Section 3(1) above. Section 3(2): Where the processor is processing personal data for a controller outside of ADGM, the processor must comply with the requirements of the Regulations to the extent possible, taking into account whether the controller is subject to similar obligations under the laws of its home jurisdiction. Section 3(3): The Regulations apply to natural persons whatever their nationality or place of residence.
Goods & servicies from abroad	
Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing Regulationsivities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	See Section 3 above.

GDPR	Regulations
Monitoring from abroad	
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	See Section 3 above.

1.3. Material scope

Fairly consistent

The Regulations differ slightly in the definitions for personal data and automated processing, although remain consistent with the GDPR definitions of data processing, pseudonymised data, and special categories of data, whilst explicitly referring to criminal data in the latter. The Regulations also do not explicitly define anonymous data or anonymisation, although it does refer to the use of anonymisation as a security measure throughout.

GDPR	Regulations
Personal data/ personal information	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fRegulationsors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 62(1): 'personal data' means any information relating to a data subject.
Data processing	
Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	Section 62(1): 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Special categories of data	
Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Section 62(1): 'Special categories of personal data' means the categories of data listed in Section 7(1) of the Regulations. Section 7(1): Processing of: • personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; • genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Please note that Section 62(1) further defines biometric data, data concerning health, and genetic data; and

GDPR	Regulations
Special categories of data (cont'd)	
	• personal data relating to criminal convictions and offences or related security measures; is prohibited.
Anonymised data	
Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	The Regulations do not explicitly define 'anonymised data.' However, the Regulations refer to the use of anonymisation as a security measure throughout. In particular, Section 31(1)(b) of the Regulations refers to personal data that is anonymised so that it no longer constitutes personal data.
Pseudonymised data	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	Section 62(1): 'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.
Automated processing	
Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	Section 2(1): The Regulations apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria do not fall within the scope of the Regulations.
General exemptions	
Article 2(2): This Regulation does not apply to the processing of personal data: (a) in the course of an Regulationsivity which falls outside the scope of Union law; (b) by the Member States when carrying out Regulationsivities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; or (c) by a natural person in the course of a purely personal or household Regulationsivity.	Section 2(2): The Regulations do not apply to the processing of personal data: • by a natural person for the purposes of purely personal or household activity; or • by public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security.

2. Key definitions

Fairly consistent

2.1. Personal data

The Regulations and the GDPR contain similar definitions, with some variation on legal terms where the Regulations clarify, for example, applicable law. The Regulations also refer explicitly to the GDPR and its supervisory authorities, despite it being outside of the EU and not directly applicable.

GDPR	Regulations
Personal data/ personal information	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fRegulationsors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 62(1): 'personal data' means any information relating to a data subject.
Special categories of data	
Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Section 62(1): 'Special categories of personal data' means the categories of data listed in Section 7(1) of the Regulations. Section 7(1): Processing of: • personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; • genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Please note that Section 62(1) further defines biometric data, data concerning health, and genetic data; and • personal data relating to criminal convictions and offences or related security measures; is prohibited.
Online identifiers	
Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.	Section 62(1): As part of the definition for 'data subject', the Regulations state that an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier, among other things.

GDPR	Regulations
Biometric Data	
Article 4(14): 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.	Section 62(1): 'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data.
Data concerning health	
Article 4(13):'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.	Section 62(1): 'Data Concerning Health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveals information about his or her health status.
Genetic Data	
Recital 34: Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained. Article 4(13): 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.	Section 62(1): 'Genetic Data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which gives unique information about the physiology or the health of that natural person and which results, in particular, from an analysis of a biological sample from the natural person in question.
GDPR	
Not applicable.	Section 62(1): 'GDPR' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, as amended from time to time.

2.2. Pseudonymisation

Fairly Consistent

As aforementioned, the Regulations do not explicitly define 'anonymisation,' although the concept is referred to throughout as an appropriate security measure alongside pseudonymisation, which is defined consistently with the GDPR.

GDPR	Regulations
Anonymisation	
Recital 26: 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	The Regulations do not explicitly define 'anonymised data.' However, the Regulations refer to the use of anonymisation as a security measure throughout. In particular, Section 31(1)(b) of the Regulations refers to personal data that is anonymised so that the it no longer constitutes personal data.
Pseudonymisation	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	Section 62(1): 'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

2.3. Controllers and processors

The Regulations build the GDPR's definitions for data controller, processor, data protection impact assessment ('DPIA'), and data protection officer ('DPO'), as well as the requirement for controller-processor contracts, into the applicable law for ADGM.

GDPR	Regulations

Data controller

Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Section 62(1): 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor

Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Section 62(1): 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Controller and processor contracts

Article 28(3): Processing by a processor shall be governed by a contrRegulations or other legal Regulations under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contract.]

Section 26(3): Processing by a processor must be governed by a contract or other legal act under applicable law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [Section 26 also goes on to stipulate necessary information to be included in such a contract].

Data Protection Impact Assessment ('DPIA')

DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).

Section 62(1): 'Data Protection Impact Assessment' ('DPIA') has the meaning given in section 34(1).

Section 34(1): The controller must, prior to Processing that is likely to result in a high risk to the rights of natural persons, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a DPIA).

GDPR	Regulations

Data Protection Officer ('DPO')

DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information).

Section 62(1): DPO has the meaning given in Section 35 of the Regulations, which sets out requirements related to DPOs (see section 5.4. below for further information).

2.4. Children

Fairly inconsistent

Where the GDPR does not define child, the Regulations offer a definition which clarifies that a child constitutes a natural person under the age of 18, in comparison to the GDPR where the age of consent is 16, and Member States may amend this to not younger than 13. Further, the Regulations do not explicitly outline requirements for consent for processing children's data. Both the GDPR and the Regulations require the provision of information to be appropriately understandable where addressing children.

GDPR	Regulations

Children's definition

The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

Section 62(1): 'Child' means a natural person under the age of 18 years old.

Consent for processing children's data

Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

The Regulations do not explicitly refer to conditions for obtaining consent to process children's data. However, Section(5)(f) states that processing is lawful only if and to the extent that, among other things, processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of the data subject which require protection of personal data, in particular where the data subject is a child.

Privacy notice (children)

Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

Section 10(1)(a): Regarding transparent information, communication and modalities for the exercise of the rights of the data subject, the controller must take appropriate measures to provide any information referred to in Sections 11 and 12 and any communication under Sections 13 to 20 and Section 32 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

2.5. Research

Fairly consistent

Although both the GDPR and the Regulations provide for research purposes as a legal basis for processing, the Regulations develop further on safeguards and conditions for the same, providing for further exceptions to the exercise of data subject rights.

GDPR	Regulations

Scientific/ historical research definition

Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.

Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

Section 62(1): 'Archiving and research purposes' means archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Section 9.

Section 7(2)(f): The prohibition of processing special categories of personal data provided under Section 7(1) does not apply if, among other things, processing is necessary for archiving and research purposes in accordance with applicable law.

Compatibility with original purpose of collection

Article 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

Section 4(3)(a): Where personal data is processed for archiving and research purposes, the processing is deemed to be compatible with the initial purposes for which the personal data was collected as required by Section 4(1)(b) of the Regulations.

Appropriate safeguards

Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of

Section 4(3)(b): Where personal data is processed for archiving and research purposes, it may be stored for longer periods than stated in Section 4(1)(e) of the Regulations, provided appropriate technical and organisational measures are used to safeguard the rights of the data subject.

Section 9: Processing for archiving and research purposes must be subject to the following safeguards:

- technical and organisational measures must be in place, in particular to ensure compliance with Section 4(1)(c), which may include pseudonymisation or anonymisation;
- the processing must not cause, or be likely to cause, substantial damage or substantial distress to a data subject; and

GDPR	Regulations
Appropriate safeguards (cont'd)	
	• the processing must not be carried out for the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purpose of medical research that has been approved by a public authority or research institution.
Data subject rights (research)	
Under Article 17(3), the right to erasure may not apply in cases of scientific or historical research. Article 21(6), however, provides that data subjects may exercise the right to object to data processing for scientific or historical research purposes. In addition, Article 89 provides that Member States may derogate from the GDPR in regard to data subject rights and data processing for research purposes.	See Section 9(1)(b) above. Under Section 12(5), the controller does not need to provide the data subject with certain information where personal data has not been obtained from the data subject, as required under Section 12(1) to 12(4), where the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving and research purposes or in so far as the obligation referred to in Section 12(1) is likely to render impossible or seriously impair the achievement of the objectives of the processing, provided that the controller takes appropriate measures to protect the data subject's rights and legitimate interests, including making the information publicly available. Similarly, under Section 15(3)(c), the right to erasure under does not apply to the extent that processing is necessary for archiving and research purposes to the extent that the right referred to in Section 15(1) is likely to render impossible or seriously impair the achievement of the objectives of that processing. Furthermore, under Section 19(5) on the right to object, where personal data is processed for archiving and research purposes, the data subject has the right to object to processing of their personal data, unless the processing is necessary for the performance of a task carried out for reasons of public interest. In summary, Section 21(4) clarifies that the obligations and rights provided for in Sections 13(1) to 13(3), Section 14, Section 16(1), Section 17, Section 18(1), and Section 19(1) will not apply to personal data processed for archiving and research purposes: • to the extent that the application of those provisions would prevent or seriously impair the achievement of those purposes; and

GDPR	Regulations
Data subject rights (research) (cont'd)	
	• provided that Sections 13(1) to 13(3) will only not apply to processing for scientific or historical research or statistical purposes where the results of the research or any resultant statistics are not made available in a form which identifies a data subject.

3. Legal basis

Fairly consistent

The Regulations do not refer to journalistic or artistic purposes for processing personal data as a legal basis, although both the GDPR and the regulations have otherwise similar legal grounds for processing personal data, including consent, contractual performance, controller obligations, and public interest. The Regulations develop within its main body on the conditions for consent.

GDPR	Regulations

Legal grounds

Article 6(1): Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contrRegulations to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contrRegulations;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is 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

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Section 5: Processing is lawful only if and to the extent that:
(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject under applicable law;
(d) processing is necessary to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out by a public authority in the interests of ADGM, or in the exercise of:
(i) ADGM's;
(ii) the Financial Services Regulatory Authority's;
(iii) the ADGM Court's; or
(iv) the Registration Authority's functions or in the exercise of official authority vested in the controller under applicable law; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or rights of the data subject which require protection of personal data, in particular where the data subject is a child.

Section 5(2): Section 5(1)(f) does not apply if processing is necessary for any of the purposes described in Section 5(1)(e).

Sensitive data (legal basis)

There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.

Section 7 provides specific requirements for processing special categories of personal data.

GDPR	Regulations

Conditions for consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Article 4: (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative Regulationsion, signifies agreement to the processing of personal data relating to him or her.

Section 6: Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they (whether in writing, electronically or orally), by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
Silence, pre-ticked boxes or inactivity do not constitute consent.
For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes for which it is intended the personal data will be processed.
Where processing is based on consent, the controller must be able to demonstrate that the data subject has consented to processing of their personal data.
If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
Any part of such a declaration which constitutes a contravention of the Regulations will not be binding.
The data subject has the right to withdraw their consent at any time. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal. The data subject must be informed of this before giving consent.
It must be as easy to withdraw consent as it is to give consent.
When assessing if consent is freely given the assessor must take into account whether:

- the data subject has a genuine or free choice or is unable to refuse or withdraw consent without detriment; and
- the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Journalism/artistic purposes

Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

The Regulations do not explicitly refer to journalistic or artistic purposes.

4. Controller and processor obligations

4.1. Data transfers

Part V of the Regulations is dedicated to transfers of personal data outside of the ADGM or to international organisations, and provides similar mechanisms as the GDPR, including standard contractual clauses ('SCCs'), binding corporate rules ('BCRs'), derogations, and adequacy, for which there is specific assessment criteria. Neither legislation requires data localisation or residency, although sectoral laws may apply.

GDPR	Regulations

Adequate protection

GDPR	Regulations
Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.	Section 41: A transfer of personal data outside of ADGM or to an International Organisation may take place where the Commissioner of Data Protection has decided that the receiving jurisdiction, one or more specified sectors within that jurisdiction, or the International Organisation in question ensures an adequate level of protection of personal data. Such a transfer will not require any specific authorisation. Section 41 goes on to clarify elements which the Commissioner of Data Protection must take into account when assessing the adequacy of the level of protection of personal data by a country or international organisation, as well as the procedure for the same.

Other mechanisms for data transfers

GDPR	Regulations
Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. (2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules in accordance with Article 47;	Section 42: In the absence of a decision pursuant to Sections 41(3) or 41(7), a controller or processor may transfer personal data to a controller or processor outside of ADGM or to an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The Commissioner of Data Protection may adopt SCCs that contain appropriate safeguards for the rights of data subjects whose personal data is being transferred, including by approving the then current standard contractual clauses issued by the European Commission, or adopted

GDPR	Regulations

Other mechanisms for data transfers (cont'd)

GDPR	Regulations
(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. (3) Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: (a) contrRegulationsual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	by a supervisory authority for the same purpose, upon which approval such standard contractual clauses will be incorporated into the Regulations by reference. The appropriate safeguards referred to in section 42(1) may be provided for, without requiring any specific authorisation from the Commissioner of Data Protection, by: (a) a legally binding and enforceable instrument between public authorities; (b) BCRs in accordance with Section 43; (c) standard data protection clauses adopted by the Commissioner of Data Protection in accordance with Section 42(2); (d) an approved code of conduct pursuant to Section 37 together with binding and enforceable commitments of the controller or Processor in the jurisdiction outside of ADGM to apply the appropriate safeguards, including as regards data subjects' rights; or (e) an approved certification mechanism pursuant to Section 39 together with binding and enforceable commitments of the controller or processor in the jurisdiction outside of ADGM to apply the appropriate safeguards, including as regards data subjects' rights. Subject to the authorisation from the Commissioner of Data Protection, the appropriate safeguards referred to in Section 42(1) may also be provided for by: (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data outside of ADGM or the international organisation; or (b) provisions to be inserted into administrative arrangements, including regulatory memorandums of understanding between public authorities or domestic or international bodies which include enforceable and effective data subject rights. Permits issued under Section 5(1)(a) of the Data Protection Regulations 2015 will remain valid as evidence of compliance with this section until amended, replaced or revoked, if necessary, by the Commissioner of Data Protection.

Data localisation

GDPR	Regulations
Not applicable.	Not applicable.

4.2. Data processing records

Fairly consistent

Controllers and processors must maintain a record of processing activities in both jurisdictions. However, the Regulations do not include exemptions to the controller or processor obligation to maintain records of processing activities and do require registration of data controllers, and notification of processing activities with the Commissioner of Data Protection, as well as data protection fees and renewal fees. The requirement for data protection fees and data processing notification to the Commissioner of Data Protection is not required for establishments employing fewer than five employees, unless it carries out high risk processing activities.

GDPR	Regulations

Data controller obligation

Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing Regulationsivities under its responsibility. That record shall contain all of the following information:

(a) the name and contRegulations details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data; and

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Section 28(1): Each controller must maintain a record of processing activities under its responsibility. That record must contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller and the DPO;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data has been or will be disclosed including recipients outside of ADGM or in international organisations;

(e) where applicable, transfers of personal data outside of ADGM or to an international organisation, including the identification of that location outside of ADGM or the international organisation and, in the case of transfers referred to section 44(1)(b), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of personal data; and

(g) where possible, a general description of the technical and organisational security measures referred to in Section 30(1).

GDPR	Regulations

Data processor obligation

Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing Regulationsivities carried out on behalf of a controller, containing:

(a) the name and contRegulations details of the processor or processors and of each controller on behalf of which the processor is Regulationsing, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
(b) the categories of processing carried out on behalf of each controller;
(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and
(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Section 28(2): Each processor must maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting and the DPO; (b) the categories of processing carried out on behalf of each controller; (c) where applicable, transfers of personal data outside of ADGM or to an international organisation, including the identification of that location outside of ADGM or the international organisation and, in the case of transfers referred to in Section 44(1)(b), the documentation of suitable safeguards; and (d) where possible, a general description of the technical and organisational security measures referred to in section 30(1).

Records format

Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

Section 28(3): The records referred to in Sections 28(1) and 28(2) must be in writing, including in electronic form.

Required to make available

Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

Section 28(4): The controller or the processor must make the record available to the Commissioner of Data Protection on request.

Exemptions

Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

The Regulations do not include exemptions to the controller or processor obligation to maintain records of processing activities.

GDPR	Regulations
General Data Processing Notification ('DPN')	
Not applicable.	Section 24: A controller must, before, or as soon as reasonably practicable after, it starts processing personal data under these Regulations: (a) pay a data protection fee to the Commissioner of Data Protection in respect of the 12 months from the date it commenced processing personal data under the Regulations; and (b) notify the Commissioner of Data Protection of: (i) its name and address (which, in the case of a registered company, will be its registered office); and (ii) the date it commenced processing personal data under these Regulations. Each year, within one month of the expiry of the anniversary on which it commenced processing personal data under these Regulations, the controller must pay a renewal fee in the amount specified by rules made by the Board to the Commissioner of Data Protection. The obligations referred to in sections 24(1) and 24(2) do not apply to an establishment employing fewer than five employees, unless it carries out high risk processing activities.

4.3. Data protection impact assessment

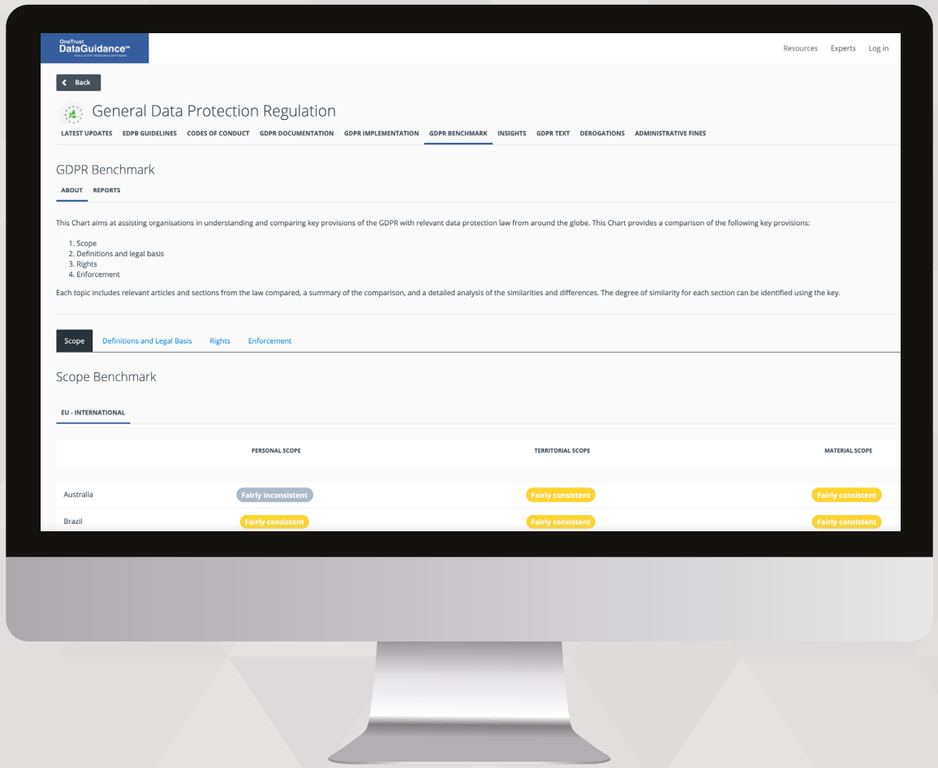
Both the GDPR and the Regulations require that controllers carry out DPIAs prior to high risk processing activities, providing a list of circumstances where the same is met. A slight terminological variation is that, in the ADGM, where the DPIA indicates that the processing activity would likely result in a high risk to the rights of natural persons, the regulator must be notified, where in the EU the authorities must be consulted.

GDPR	Regulations
When is a DPIA required	
Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. [...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.	Section 34(1) to (4): The controller must, prior to processing that is likely to result in a high risk to the rights of natural persons, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'Data Protection Impact Assessment'). A single DPIA may address a set of similar processing operations that present similar high risks. The outcome of the DPIA should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with these Regulations. The controller must seek the advice of the DPO, where designated, when carrying out a DPIA. The Commissioner of Data Protection must publish a list of the kind of processing operations which are subject to the requirement for a DPIA pursuant to Section 34(1) and may review this list from time to time. Section 34(6): Where necessary, the controller must carry out a review to assess if processing is performed in accordance with the DPIA including when there is a change of the risk represented by processing operations. Section 62(1) defines high-risk processing activities as follows: 'High Risk Processing Activities' means the processing of personal data where one or more of the following applies: (a) a considerable volume of personal data will be processed; (b) the processing is likely to result in a high risk to the rights of data subjects; (c) the processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (d) the processing includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a data subject or renders it more difficult for a data subject to exercise

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk, and achieve global compliance



Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China
and 20+ other global laws & frameworks

Understand and compare key provisions of the GDPR with relevant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions

- Scope
- Rights
- Definitions and legal basis
- Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

GDPR	Regulations

When is a DPIA required (cont'd)

	their rights; or (e) the processing includes special categories of personal data, except where processing of such data is required by applicable law.

DPIA content requirements

Article 35(7): The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	Section 34(5): The DPIA must: (a) describe the nature, scope, context and purpose of the processing; (b) assess necessity, proportionality, and compliance measures; (c) identify and assess risks to individuals; and (d) identify any additional measures to mitigate the risks identified.

Consultation with authority

Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36 goes on to detail requirements related to such prior consultation].	Section 34(7): The controller must notify the Commissioner of Data Protection prior to carrying out any processing where a DPIA indicates that the processing would be likely to result in a high risk to the rights of natural persons. The notification must contain information in Section 34(5).

4.4. Data protection officer appointment

Sections 35 to 37 of the Regulations deal with the designation, position, and tasks of the DPO, in a highly consistent manner as within the GDPR. However, the Regulations specify, among other things, that the DPO's appointment must be notified to the regulator within one month, while the GDPR does not provide for a specific deadline.

GDPR	Regulations

DPO tasks

Article 39(1): The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; and (e) to Regulations as the contRegulations point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	Section 37(1) and (2): The tasks of the DPO include: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the Regulations and to other data protection provisions under applicable law; (b) to monitor compliance with the Regulations, with other data protection provisions under applicable law and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the DPIA and monitor its performance pursuant to Section 34; (d) to cooperate with the Commissioner of Data Protection; and (e) to act as the contact point for the Commissioner of Data Protection on issues relating to processing and to consult with the Commissioner of Data Protection, where appropriate, with regard to any other matter. The DPO must in the performance of their tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

When is a DPO required

Article 37(1): The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts Regulationsing in their judicial capacity; (b) the core Regulationsivities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or	Section 35(1): The controller and the processor must appoint a person to perform the tasks listed in Section 37 (a 'DPO') where: (a) the processing is carried out by a public authority, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of data subjects on a large scale; or

GDPR	Regulations

When is a DPO required (cont'd)

GDPR	Regulations
(c) the core Regulationsivities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.	(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data. Section 35(2): A DPO: (a) may be appointed in respect of a single entity, a group or multiple, independent entities; (b) may perform additional roles in respect of a controller or processor in addition to performing the role of DPO; (c) does not need to be an employee of the relevant controller or processor provided it enters into an agreement in writing with the controller, or processor, as the case may be; and (d) does not need to be resident within ADGM, in each case, provided that the DPO is easily accessible by each entity it acts for, and no other role held by the DPO conflicts or is likely to conflict with the DPO's obligations under the Regulations.

Group appointments

Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	Section 35(2)(a): A DPO: (a) may be appointed in respect of a single entity, a group or multiple, independent entities [...]. Section 62(1): 'Group' has the meaning given to that term in the Commercial Licensing Regulations 2015 (Controlled Activities) Rules 2015.

Notification of DPO

Article 37(7): The controller or the processor shall publish the contRegulations details of the data protection officer and communicate them to the supervisory authority.	Section 35(4): The controller or the processor must notify the Commissioner of Data Protection within one month following the appointment or resignation of any DPO. The notification must include the contact details of the new DPO and, in the case of a resignation, reasons for the resignation.

Qualifications

Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and prRegulationsices and the ability to fulfil the tasks referred to in Article 39.	Section 35(3): The DPO must be appointed on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Section 37.

4.5. Data security and data breaches

The GDPR and the Regulations contain consistent requirements for data breach notification to data subjects and the relevant authority, within the same timeframes, as well as consistent provisions on security measures that controllers and processor must implement.

GDPR	Regulations

Security measures defined

GDPR	Regulations
Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (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; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Section 30(1), (2), and (3): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights of natural persons, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate: (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. In assessing the appropriate level of security the controller and processor must take into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. The controller and processor must take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process it except on instructions from the controller, unless they are required to do so by applicable law.

Data breach notification to authority

Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	Section 32(1): In the case of a personal data breach, the controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner of Data Protection, unless the personal data breach is unlikely to result in a risk to the rights of natural persons. Where the notification to the Commissioner of Data Protection is not made within 72 hours, it must be accompanied by reasons for the delay.

GDPR	Regulations

Timeframe for breach notification

GDPR	Regulations
See Article 33(1) above.	See Section 32(1) above.

Notifying data subjects of data breach

GDPR	Regulations
Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	Section 33(1): When the personal data breach is likely to result in a high risk to the rights of natural persons, the controller must communicate the personal data breach to the data subject without undue delay.

Data processor notification of data breach

GDPR	Regulations
Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	Section 32(2): The processor must notify the controller without undue delay after becoming aware of a personal data breach.

Exceptions

GDPR	Regulations
Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	Section 33(3): The communication to the data subject referred to in Section 33(1) is not required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights of data subjects referred to in Section 33(1) is no longer likely to materialise; or (c) it would involve disproportionate effort (having regard to the number of data subjects, the age of the data and any appropriate safeguards adopted). In such a case, there must instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4.6. Accountability

Whereas the GDPR explicitly defines 'accountability,' the Regulations do not, although its description of the concept of controller responsibility under Section 4(2) is otherwise consistent. Section 59 of the Regulations is dedicated to in depth clarifications of controller and processor liabilities.

GDPR	Regulations

Principle of accountability

GDPR	Regulations
Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). [Paragraph 1 details principles of: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.]	The Regulations do not explicitly refer to the principle of accountability. However, Section 1(e) outlines that the objects of the Regulations include establishing the primary responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf. Furthermore, Section 4(2) provides that the controller is responsible for, and must be able to demonstrate compliance with, Section 4(1). [Section 4(1) details principles for processing personal data].

Liability of data controllers and data processors

GDPR	Regulations
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has Regulationsed outside or contrary to lawful instructions of the controller.	Section 59(2) and (3): Any controller involved in processing is liable for the damage caused by processing which contravenes the Regulations. A processor is liable for the damage caused by processing only where it has not complied with obligations of these Regulations specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

5. Rights

5.1. Right to erasure

Both the GDPR and the Regulations provide for the right to erasure, with similar exceptions for the same. However, the GDPR provides an additional legal ground for the exercise of the right when personal data have been collected in relation to the offer of information society services, as well as an additional exception to the right to erasure where the processing is necessary for exercising the right of freedom of expression and information. The GDPR and the Regulations also present slight differences in relation to response timeframes, with the Regulations requiring controllers to reply within two months, with the possibility of extending the period of one additional month, while the GDPR provides for an initial one month deadline, with the possibility of extending the same of two months.

GDPR	Regulations

Grounds for erasure

Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Section 15(1): The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller has the obligation to erase personal data without undue delay where one of the following applies: (a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to Section 5(1)(a) or 7(2)(a), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Section 19(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Section 19(3); (d) the personal data has been unlawfully processed; or (e) the personal data has to be erased for compliance with a legal obligation in applicable law to which the controller is subject.

GDPR	Regulations

Inform data subject of right

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Section 10(1): The controller must take appropriate measures to provide any information referred to in Sections 11 and 12 and any communication under Sections 13 to 20 and Section 32 relating to processing to the data subject: (a) in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child; and (b) in writing, electronically or, if requested by the data subject, orally as long as that data subject has provided proof of their identity.

Fees

Article 12(5): Information provided under Articles 13 and 14 and any communication and any Regulationsions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive charRegulationser, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the Regulationsion requested; or (b) refuse to Regulations on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive charRegulationser of the request.

Section 10(6): Information provided under Sections 11 and 12 and any communication and any actions taken under Sections 13 to 20 and Section 33 must be provided free of charge. Where requests from a data subject are unreasonable or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller bears the burden of demonstrating the unreasonable or excessive character of the request.

Response timeframe

Article 12(3): The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Section 10(3) and (4): Subject to Section 10(4), the controller must provide information on action taken on a request under Sections 13 to 20 to the data subject without undue delay and in any event within two months of receipt of the request. Where the data subject makes the request by means of an electronic form, the information may be provided by electronic means where possible, unless otherwise requested by the data subject.
The period referred to in Section 10(3) may be extended by one month, where necessary, taking into account the complexity and number of the requests including any related requests received by the controller whether or not from the same data subject. The controller must inform the data subject of any such extension within two months of receipt of the request, together with the reasons for the delay.

GDPR	Regulations

Format of response

GDPR	Regulations
Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	Section 10(1)(b): The controller must take appropriate measures to provide any information referred to in Sections 11 and 12 and any communication under Sections 13 to 20 and Section 32 relating to processing to the data subject: [...] (b) in writing, electronically or, if requested by the data subject, orally as long as that data subject has provided proof of their identity. Section 10(3): Where the data subject makes the request by means of an electronic form, the information may be provided by electronic means where possible, unless otherwise requested by the data subject.

Publicly available data

GDPR	Regulations
Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	Section 15(2): Where the controller has made the personal data public and is obliged pursuant to Section 15(1) to erase the personal data, the controller, taking account of available technology and the cost of implementation, must take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, that personal data.

Exceptions

GDPR	Regulations
Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or	Section 15(3) and (4): Sections 15(1) and 15(2) will not apply to the extent that processing is necessary: (a) for compliance with a legal obligation which requires processing under applicable law to which the controller is subject or for the performance of a task carried out by a public authority in the interests of ADGM, or in the exercise of (i) ADGM's; (ii) the Financial Services Regulatory Authority's; (iii) the ADGM Court's; and (iv) the Registration Authority's functions or in the exercise of official authority vested in the controller; (b) for reasons of public interest in the area of public health in accordance with Sections 7(2)(d) and 7(2)(e); (c) for archiving and research purposes to the extent that the right referred to in Section 15(1) is likely to render impossible or seriously impair the achievement of the objectives of that processing, or (d) for the establishment, exercise or defence of legal claims.

GDPR	Regulations

Exceptions (cont'd)

GDPR	Regulations
(e) for the establishment, exercise or defence of legal claims. Article 12(5): Information provided under Articles 13 and 14 and any communication and any Regulationsions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive charRegulationser, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the Regulationsion requested; or (b) refuse to Regulations on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive charRegulationser of the request. The The Regulations does not provide specific exceptions to a right to erasure.	Where erasure of personal data is not feasible for technical reasons, then the controller is not in violation of the Regulations for failing to comply with a request for erasure of the personal data under Section 15(1), if: (a) the controller collected the personal data from the data subject; and (b) the information provided to the data subject under Section 11(2)(h) was explicit, clear and prominent with respect to the manner of processing the personal data and expressly stated that erasure of the personal data at the request of the data subject would not be feasible.

5.2. Right to be informed

Fairly consistent

The right to be informed is overall consistent between the GDPR and the Regulations. One of the differences include the addition within the Regulations of a requirement for the controller to provide specific further information if the controller intends to process personal data in a manner that will restrict or prevent the data subject from exercising their rights to request rectification or erasure of personal data, or to object to the processing of the personal data.

GDPR	Regulations

Informed prior to/ at collection

Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a) the identity and the contRegulations details of the controller and, where applicable, of the controller's representative;
(b) the contRegulations details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fRegulations that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contrRegulationsual requirement, or a requirement necessary to enter into a contrRegulations, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Section 11: Where personal data relating to a data subject is collected from the data subject, the controller must, at the time when personal data is obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller; (b) the contact details of the DPO, where applicable; (c) the purposes of the processing for which the personal data is intended as well as the legal basis for the processing; (d) where the processing is based on Section 5(1)(f), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; and (f) where applicable, the fact that the controller intends to transfer personal data to a recipient outside of ADGM or to an international organisation and: (i) the existence or absence of an adequacy decision by the Commissioner of Data Protection; or (ii) in the case of transfers referred to in Sections 42, 43, or Section 44(1)(b), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
In addition to the information referred to in Section 11(1), the controller must, at the time when personal data is obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the rights set out in Sections 13 to 16, 18, and 19; (c) where the processing is based on either of Sections 5(1)(a) or 7(2)(a): (i) the existence of the right to withdraw consent at any time; and (ii) that the lawfulness of any processing based on consent prior to that withdrawal will not be affected by the subsequent withdrawal of consent; (d) the right to lodge a complaint with the Commissioner of Data Protection; (e) whether the provision of personal data is a requirement under applicable law, a contractual requirement, or a requirement necessary to enter into a contract; (f) whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data; (g) the existence of automated decision-making, including profiling, referred to in Sections 20(1) and 20(4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and (h) if the controller intends to process personal data in a manner that will restrict or prevent the data subject from exercising their rights to request rectification or erasure of personal data in accordance with Sections 14(1) or 15(1), or to object to the processing of the personal data in accordance with Section 19. In such cases, the controller must: (i) include a clear and explicit explanation of the expected impact on such rights; and (ii) satisfy itself that the data subject understands and acknowledges the extent of any such restrictions. (3) Where the controller intends to further process the personal data for a purpose other than that for which the personal data was collected, the controller must provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in Section 11(2).

What information is to be provided

See Article 13(1) and (2) above.

See Section 11 above.

When data is from third party

In addition to the information required under Article 13, Article 14(2) replaces the requirement that data subjects are provided with information on the legitimate interests pursued by the controller or by a third party, with an obligation to inform data subjects of the categories of personal data. Furthermore, paragraph (e) of Article 13(2) is replaced with a requirement to inform data subjects of the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources.

Section 12 pertains to information to be provided where personal data has not been obtained from the data subject.

GDPR	Regulations

Intelligibility requirements

GDPR	Regulations
Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	Section 10(1): The Ccontroller must take appropriate measures to provide any information referred to in Sections 11 and 12 and any communication under Sections 13 to 20 and Section 32 relating to processing to the data subject: (a) in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child; and (b) in writing, electronically or, if requested by the data subject, orally as long as that data subject has provided proof of their identity.

Format

GDPR	Regulations
See Article 12(1) above.	See Section 10(1) above.

Exceptions

GDPR	Regulations
The requirements of Article 13 do not apply where the data subject already has the information. The requirements of Article 14 do not apply where: (a) the data subject already has the information; (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.	Section 11(4): Sections 11(1), 11(2), and 11(3) do not apply to the extent that the data subject already has the information. Section 12(5): Sections 12(1) to 12(4) do not apply to the extent that: (a) the data subject already has the information; (b) the provision of such information proves impossible or would involve a disproportionate effort (having regard to the number of data subjects, the age of the data and any appropriate safeguards adopted), in particular for processing for archiving and research purposes or in so far as the obligation referred to in Section 12(1) is likely to render impossible or seriously impair the achievement of the objectives of that processing, provided that the controller takes appropriate measures to protect the data subject's rights and legitimate interests, including making the information publicly available; (c) obtaining or disclosure is expressly required by applicable law which provides appropriate measures to protect the data subject's legitimate interests; or (d) where the personal data must remain confidential subject to an obligation of professional secrecy, or duty of confidentiality, regulated by applicable law.

5.3. Right to object

The right to object to processing activities generally and in the context of direct marketing, the right to restriction of processing, and conditions for consent withdrawal are all provided within both the GDPR and the Regulations.

GDPR	Regulations

Grounds for right to object/ opt out

GDPR	Regulations
Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	Section 19(1) and (2): A data subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data, which is based on Sections 5(1)(e) and 5(1)(f), including profiling based on those provisions. Where the data subject objects to the processing of their personal data, the controller must not process the personal data unless the controller reasonably considers that: (a) there are legitimate grounds for the processing which override the interests or rights of the data subject; or (b) the processing is necessary for the establishment, exercise or defence of legal claims.

Withdraw consent

GDPR	Regulations
Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	Section 6(7), (8), and (9): The data subject has the right to withdraw their consent at any time. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal. The data subject must be informed of this before giving consent. It must be as easy to withdraw consent as it is to give consent. When assessing if consent is freely given the assessor must take into account whether: (a) the data subject has a genuine or free choice or is unable to refuse or withdraw consent without detriment; and (b) the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Restrict processing

GDPR	Regulations
Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:	Section 16: The data subject has the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for

GDPR	Regulations
Restrict processing (cont'd)	
(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.	a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims; or (d) the data subject has objected to processing pursuant to Section 19(1) pending the verification whether the legitimate grounds of the controller override those of the data subject. Where processing has been restricted under Section 16(1), such personal data must, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. The controller must inform a data subject who has obtained restriction of processing pursuant to Section 16(1) before the restriction of processing is lifted.
Object to direct marketing	
Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	Section 19(3) and (4): where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing, including profiling, of their personal data for such direct marketing purposes. Where the data subject objects to processing for direct marketing purposes, the personal data must not be processed for such purposes.
Inform data subject of right	
See Article 12(1) in section 5.1. above. In addition, Article 21(4) provides: At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	See Section 11 and 12 in section 5.1. above. In addition, Section 19(6) provides: No later than the time of the first communication with the data subject, the right referred to in Sections 19(1) and 19(3) must be explicitly brought to the attention of the data subject and must be presented clearly and separately from any other information.

GDPR	Regulations
Fees	
See Article 12(5) in section 5.1. above.	See Section 10(6) in section 5.1. above.
Response timeframe	
See Article 12(3) in section 5.1. above.	See Section 10(3) and (4) in section 5.1. above.
Format of response	
See Article 12(1) in section 5.1. above.	See Section 10(1)(b) and (3) in section 5.1. above.
Exceptions	
See Article 12(5) in section 5.1. above.	Section 19(5): Where personal data is processed for archiving and research purposes the data subject has the right to object to processing of their personal data, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

5.4. Right of access

The right of access is provided overall consistently between the GDPR and the Regulations. The Regulations contain additional stipulations on fees for the request of additional copies by the data subject and on the verification of the data subject.

GDPR	Regulations

Grounds for right of access

Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.

Article 13(1): A data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed.

Information to be accessed

Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source; and
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Article 13(1): a data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to the personal data and the following information:
(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients outside of ADGM or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with the Commissioner of Data Protection;
(g) where the personal data is not collected from the data subject, any available information as to its source; and
(h) the existence of automated decision-making, including profiling, referred to in Sections 20(1) and 20(4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
Furthermore, Section 13(2) provides: Where personal data is transferred outside of ADGM or to an international organisation, the data subject has the right to be informed of the appropriate safeguards pursuant to Section 41 relating to the transfer.

GDPR	Regulations

Inform data subject of right

See Article 12(1) in section 5.1.

See Section 10(1) in section 5.1. above.

Fees

See Article 12(5) in section 5.1. above.

Section 13(3): The controller must provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information must be provided in a commonly used electronic form.

Verify data subject request

Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

Section 8: If the purposes for which a controller processes personal data do not or no longer require the identification of a data subject by the controller, the controller is not obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with these Regulations.
Where, in cases referred to in Section 8(1), the controller is able to demonstrate that it is not in a position to identify the data subject, the controller must inform the data subject accordingly, if possible.
In such cases, Sections 13 to 18 will not apply except where the data subject, for the purpose of exercising their rights under those sections, provides additional information enabling their identification.

Response timeframe

See Article 12(3) in section 5.1. above.

See Section 10(3) in section 5.1. above.

Format of response

See Article 12(1) in section 5.1. above.

See Section 10(1) in section 5.1. above.

Exceptions

See Article 12(5) in section 5.1. above.

Section 13(4) and (5): The right to obtain a copy referred to in Section 13(3) must not adversely affect the rights of others.

5.5. Right not to be subject to discrimination

Despite neither the GDPR or the Regulations explicitly provides for a right not to be subject to discrimination, this can be implicitly deferred from the content of each legislation. Concurrently, the right not to be subject to a decision based solely on automated processing exists in both.

GDPR	Regulations

Definition of right

GDPR	Regulations
The GDPR only implies this right and does not provide an explicit definition for it.	The Regulations do not explicitly provide a right not to be subject to discrimination, although it is implied through its objectives.

Automated processing

GDPR	Regulations
Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]	Section 20: (1) The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her. [Section 20 goes on to detail this right, including exceptions].

5.6. Right to data portability

Both the GDPR and the Regulations provide for the right to data portability, with considerations for exceptions and technical feasibility of the same.

GDPR	Regulations

Grounds for portability

GDPR	Regulations
Article 20(1): The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contrRegulations pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.	Section 18(1): The data subject has the right to receive the personal data that is held by, or on behalf of, the controller concerning them, which they have provided to a controller, in a structured, commonly used, and machine-readable format and has the right to transmit that data to another controller without hindrance from the controller to which the personal data has been provided, where: (a) the processing is based on consent pursuant to Section 5(1)(a) or 7(2)(a) or on a contract pursuant to Section 5(1)(b); and (b) the processing is carried out by automated means.

Inform data subject of right

GDPR	Regulations
See Article 12(1) in section 5.1.	See Section 10(1) in section 5.1.

Fees

GDPR	Regulations
See Article 12(5) in section 5.1. above.	See Section 10(6) in section 5.1.

Response timeframe

GDPR	Regulations
See Article 12(3) in section 5.1. above.	See Section 10(3) in section 5.1.

Format

GDPR	Regulations
See Article 20(1) above.	See Section 18(1) above.

Controller to controller

GDPR	Regulations
Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	Section 18(2): A data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible.

GDPR	Regulations
Technically feasible	
See Article 20(2) above.	See Section 20(2) above.
Exceptions	
See Article 12(5) in section 5.1. above.	Section 18(3): Section 18(1) does not apply to any processing that is carried out in reliance on Section 5(1)(e). Section 18(4): The right in Section 18(1) must not adversely affect the rights of others.

6. Enforcement

6.1. Monetary penalties

Despite both the GDPR and the Regulations providing for monetary penalties and specifying mitigating factors, the Regulations provide an absolute cap of $28 million, where the GDPR adopts a two-tier approach with regard to percentages of turnover. Since data protection and renewal fees are required in the ADGM, the Regulations also sanction failure to pay the same.

GDPR	Regulations
Provides for monetary penalties	
The GDPR provides for monetary penalties.	The Regulations provide for monetary penalties.
Issued by	
Article 58(2) Each supervisory authority shall have all of the following corrective powers: [...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.	Section 50(5)(i): The corrective powers of the Commissioner of Data Protection include the power to: [...] impose an administrative fine pursuant to Section 55, in addition to, or instead of, measures referred to in this subsection, depending on the circumstances of the individual case.
Fine maximum	
Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). (6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	Section 55(1): Where a controller or processor (i) does an act or thing that it is prohibited from doing; or (ii) omits to do an act or thing that it must do by or under: (a) any Direction issued by the Commissioner of Data Protection under Section 54; (b) these Regulations; or (c) any rules made pursuant to these Regulations, the Commissioner of Data Protection, by written notice (a 'Penalty Notice') to the controller or processor, may impose a fine in respect of the contravention of such amount as the Commissioner of Data Protection determines to be appropriate, taking into account the factors in Section 55(3). The amount determined by the Commissioner of Data Protection must not exceed $28 million. Section 56(1) and (2): If a controller fails to pay the Data Protection Fee or the Renewal Fee in accordance with Section 24, the Commissioner of Data Protection may issue a monetary penalty, imposing a fine on the controller of up to 150% of the Data Protection Fee, or Renewal Fee, in addition to the Data Protection Fee, or Renewal Fee, as the case may be. The amount of the penalty for a failure to pay the Data Protection Fee in accordance with Section 24 must be specified by rules made by the Board.

GDPR	Regulations

Percentage of turnover

Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year.	The Regulations do not refer to fines in relation to percentage of turnover. See Section 55(1) above.

Mitigating factors

Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; (b) the intentional or negligent charRegulationser of the infringement; (c) any Regulationsion taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (g) the categories of personal data affected by the infringement; (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and (k) any other aggravating or mitigating fRegulationsor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.	Section 55(3): When deciding whether to impose a fine and deciding on the amount of the fine in each individual case, the commissioner of data protection may consider the following factors: (a) the nature, gravity and duration of the contravention taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected, and the level of damage suffered by them; (b) the intentional or negligent character of the contravention; (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Sections 23 and 30; (e) any relevant previous contraventions of these Regulations or the Data Protection Regulations 2015 by the controller or processor; (f) degree of cooperation with the Commissioner of Data Protection, in order to remedy the contravention and mitigate its possible adverse effects; (g) the categories of personal data affected by the contravention; (h) the manner in which the contravention became known to the Commissioner of Data Protection, in particular whether, and if so to what extent, the controller or processor notified the Commissioner of Data Protection of the contravention; (i) where measures referred to in Section 50(5) have previously been ordered against the controller or processor concerned in relation to the same subject matter, compliance with those measures; (j) adherence to approved codes of conduct pursuant to Section 38 or approved certification mechanisms pursuant to Section 39; and (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the contravention.

GDPR	Regulations

Imprisonment

Not applicable.	Not applicable.

DPO liability

Not applicable.	Not applicable

6.2. Supervisory authority

Fairly consistent

Under the GDPR, Member States may provide one or more independent public authority as the supervisory authority. Similarly, under the Regulations in the ADGM, the Board of the ADGM assigns competency to the Registrar to oversee the independent data protection supervisory authority, the Office of Data Protection, which is led by an appointed Commissioner of Data Protection.

GDPR	Regulations

Provides for data protection authority

Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

Section 47(1): The Board will: (a) assign to the Registrar the competency to oversee the administration and operation of the Office for Data Protection as an independent data protection supervisory authority; (b) appoint a person to be the Commissioner of Data Protection in accordance with Section 47(2).
Section 47(6): The Commissioner of Data Protection is responsible for the monitoring and enforcing the application of the Regulations in order to protect the rights of natural persons in relation to processing of personal data in ADGM.

Investigatory powers

Article 58(1): Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
(b) to carry out investigations in the form of data protection audits;
(c) to carry out a review on certifications issued pursuant to Article 42(7);
(d) to notify the controller or the processor of an alleged infringement of this Regulation;
(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

Section 50(1): The investigative powers of the Commissioner of Data Protection include the powers to:
(a) order, by notice in writing, controllers and processors to provide any information it reasonably requires for the performance of its duties and functions;
(b) initiate investigations into a controller's or processor's compliance with the Regulations;
(c) appoint one or more competent persons to conduct an investigation on its behalf into a controller's or processor's compliance with these Regulations. The Commissioner of Data Protection, and any person appointed under this Section 49(1)(c) must give the controller or processor (as the case may be) written notice of the decision to investigate unless the Commissioner of Data Protection believes that would likely result in the investigation being frustrated;
(d) carry out investigations in the form of data protection audits;
(e) carry out a review on certifications issued pursuant to Section 39;
(f) notify controllers and processors of any alleged contravention of these Regulations;
(g) obtain, by notice in writing, from controllers and processors, access to all personal data and to all information reasonably necessary for the performance of its duties and functions; and

GDPR	Regulations

Investigatory powers (cont'd)

(f) notify controllers and processors of any alleged contravention of these Regulations;
(g) obtain, by notice in writing, from controllers and processors, access to all personal data and to all information reasonably necessary for the performance of its duties and functions; and
(h) subject to Section 50(3) obtain access to any premises of controllers and processors, including to any data processing equipment and means, in accordance with applicable law and to search and take possession of any relevant documents or information.

Corrective powers

Article 58(2): Each supervisory authority shall have all of the following corrective powers:
(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
(e) to order the controller to communicate a personal data breach to the data subject;
(f) to impose a temporary or definitive limitation including a ban on processing;
(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such Regulationsions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

Section 50(5): The corrective powers of the Commissioner of Data Protection include the power to:
(a) issue and publish directions and warnings and make recommendations to controllers and processors that intended processing operations are likely to contravene provisions of these Regulations;
(b) issue and publish directions and reprimands to controllers and processors where processing operations have contravened provisions of these Regulations;
(c) order controllers and processors to comply with a data subject's requests to exercise his or her rights pursuant to the Regulations;
(d) order controllers and processors to bring processing operations into compliance with the provisions of the Regulations, where appropriate, in a specified manner and within a specified period;
(e) order a controller to communicate a personal data breach to the data subject;
(f) impose a temporary or permanent limitation (including a ban) on processing;
(g) order the rectification or erasure of personal data or restriction of processing pursuant to Sections 14, 15, and 16 and the notification of such actions to recipients to whom the personal data has been disclosed pursuant to Sections 15(2) and 17;
(h) withdraw a certification if the requirements for the certification are not or are no longer met;
(i) impose an administrative fine pursuant to Section 55, in addition to, or instead of, measures referred to in this subsection, depending on the circumstances of the individual case;

GDPR	Regulations

Corrective powers (cont'd)

	(j) order the suspension of data flows to a Recipient inside or outside of ADGM or to an international organisation; and (k) where appropriate, refer contraventions of the Regulations to the attention of the Court and where appropriate, commence legal proceedings, in order to enforce the provisions of the Regulations.

Authorisation/ advisory powers

Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers: (a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36; (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data; (c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation; (d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5); (e) to accredit certification bodies pursuant to Article 43; (f) to issue certifications and approve criteria of certification in accordance with Article 42(5); (g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2); (h) to authorise contrRegulationsual clauses referred to in point (a) of Article 46(3); (i) to authorise administrative arrangements referred to in point (b) of Article 46(3); (j) to approve binding corporate rules pursuant to Article 47.	Section 50(6): The authorisation and advisory powers of the Commissioner of Data Protection include the powers to: (a) issue, on its own initiative or on request, opinions to the Board, the Registrar or, in accordance with applicable law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data; (b) prepare and publish guidance on the Regulations; (c) prescribe forms to be used for any of the purposes of the Regulations; (d) approve draft codes of conduct in accordance with Section 38; (e) issue certifications and approve criteria of certification in accordance with Section 39; (f) adopt standard data protection clauses referred to in Sections 26(6) and 42(2); (g) authorise contractual clauses referred to in Section 42(4); (h) advise the Board in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with these Regulations and in particular to mitigate the risk involved for the data subject; (i) prepare and publish a list (to be updated from time to time) of processing activities that it considers require a DPIA in accordance with Section 34; and (j) approve BCRs pursuant to Section 43.

GDPR	Regulations

Tasks of authority

Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (a) monitor and enforce the application of this Regulation; (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention; (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing; (d) promote the awareness of controllers and processors of their obligations under this Regulation; (e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end; (f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation; (h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority; (i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; (j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2); (k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4); (l) give advice on the processing operations referred to in Article 36(2);	Section 49: The Commissioner of Data Protection has such powers, duties and functions as conferred on it under the Regulations and must exercise those powers and perform those duties and functions in pursuit of the objectives of the Regulations. The Commissioner of Data Protection must: (a) monitor and enforce the application of the Regulations; (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing; (c) advise the Board, ADGM, Financial Services Regulatory Authority, ADGM Courts, the Registration Authority and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights with regard to processing, in accordance with applicable law; (d) promote the awareness of controllers and processors of their obligations under the Regulations; (e) provide the public with opportunities to provide views on the activities of the Office of Data Protection; (f) handle complaints lodged by a data subject, and investigate, to the extent appropriate, the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation is necessary; (g) cooperate with, including sharing information and provide mutual assistance to, other data protection authorities with a view to facilitating the effective enforcement of legislation for the protection of personal data; (h) conduct investigations on the application of the Regulations; (i) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and business practices; (j) adopt or authorise SCCs referred to in Section 26(6) and 42(2); (k) establish and maintain a list in relation to the requirement for DPIA pursuant to Section 34(4); (l) take into account the specific needs of small and medium sized establishments in the application of the Regulations; (m) approve codes of conduct which provide sufficient safeguards pursuant to Section 38(1); (n) approve the criteria of certification pursuant to Section 39(1); (o) authorise contractual clauses and provisions referred to in Section 40(4);

GDPR	Regulations

Tasks of authority (cont'd)

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(r) authorise contrRegulationsual clauses and provisions referred to in Article 46(3);
(s) approve binding corporate rules pursuant to Article 47;
(t) contribute to the Regulationsivities of the Board;
(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
(v) fulfil any other tasks related to the protection of personal data.

(p) approve BCRs pursuant to Section 43;
(q) keep internal records of contraventions of the Regulations and of measures taken in accordance with Section 50(5);
(r) collect Data Protection Fee and Renewal Fee payments and notifications by controllers in accordance with Section 24; and
(s) fulfil any other tasks related to the protection of personal data within ADGM.
The Commissioner of Data Protection is not competent to supervise processing operations of the Court acting in its judicial capacity.
The Commissioner of Data Protection and its officers and Staff:
(a) are subject to a duty of professional secrecy or duty of confidentiality both during and after their term of office in respect of any confidential information which they become aware of in the course of the performance of their duties and functions or exercise of their powers; and
(b) during their term of office must not engage in any political activity nor any activity which would create a conflict of interest with the work of the Office of Data Protection.

Annual report

Article 59: Each supervisory authority shall draw up an annual report on its Regulationsivities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

Section 53: As soon as practicable after 1 January each year, the Commissioner of Data Protection must deliver to the Board a report on the management of the administrative affairs of the Commissioner of Data Protection for the previous year.
This report must include a list of types of contraventions addressed by the Commissioner of Data Protection in the previous year and the measures taken in response.
Such report must give a true and fair view of the state of the Commissioner of Data Protection's regulatory operations in ADGM, and its financial statements as at the end of the relevant financial year.
This report must be made available to the public.

6.3. Civil remedies for individuals

Fairly consistent

Although both the GDPR and the Regulations provide for civil remedies for individuals, the GDPR is more specific in the methods for the same, where the Regulations offer more detail on material and non-material damages which can be claimed and spotlight a focus on effective judicial remedy as an over-arching objective from the outset.

GDPR	Regulations

Provides for claims/ cause of Regulationsion

Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Section (1)(g) of the Regulations state that the objects of the Regulations include providing a means for individuals to complain about an alleged infringement of their rights relating to their personal data and to receive an effective judicial remedy.

Material and non-material damage

Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Section 59: Any person who has suffered material or non-material damage as a result of a contravention of these Regulations is entitled to compensation from the controller or processor for the damage suffered. Any compensation is in addition to, and will not limit, any fine imposed on the same controller or processor under Section 55.
Any controller involved in processing is liable for the damage caused by processing which contravenes the Regulations.
A processor is liable for the damage caused by processing only where it has not complied with obligations of these Regulations specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.
A controller or processor is exempt from liability under Section 59(2) and 59(3) if it proves that it is not in any way responsible for the event giving rise to the damage.
It is a defence to a claim brought under Section 59(2) for the controller or processor to prove that it had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned.
Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each controller or processor will be held jointly and severally liable for the entire damage in order to ensure effective compensation of the data subject.

GDPR	Regulations
Material and non-material damage (cont'd)	
	Where a controller or processor has, in accordance with Section 59(6), paid full compensation for the damage suffered, that controller or processor is entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in Section 59(2) and 59(3). Proceedings for exercising the right to receive compensation must be brought before the Court. A data subject may apply to the Court for an order that is binding on the controller, or processor, to take, or refrain from taking, specified steps in order to comply with these Regulations.
Mandate for representation	
Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is Regulationsive in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.	The Regulations do not explicitly provide a mandate for representation. However, under Section 57(2), where multiple data subjects are affected by the same alleged contravention, they may raise such complaint collectively, including via a representative body.
Specifies amount for damages	
Not applicable.	Not applicable.
Processor liability	
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.	See Section 59 above.

GDPR	Regulations
Exceptions	
Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.	See Section 59(4) above.