MÜNCHENER RÜCKVERSICHERUNGS-GESELLSCHAFT
AKTIENGESELLSCHAFT IN MÜNCHEN

Binding Corporate Rules for the Processing of EEA Data by Munich Re Group Members

Table of Contents

1. Introduction ... **3**
2. Scope of the Binding Corporate Rules ... **3**
3. Definitions and References ... **3**
4. General Data protection principles ... **3**
5. Legal basis for Processing of EEA Data ... **3**
6. Legal basis for Processing of Sensitive EEA Data ... **4**
7. Accountability ... **4**
8. Rights of Data Subjects ... **4**
9. Data security ... **5**
10. Third Country laws and practices assessment ... **5**
11. Third Country government access requests ... **6**
(a) Notification ... 6
(b) Review of legality and data minimisation ... 6
12. Relationships with Data Processors ... **7**
13. Restriction on Transfers and onward Transfers outside the Munich Re Group to and in Third Countries ... **7**
14. Liability ... **7**
15. Transparency and easy access to BCR for Data Subjects ... **8**
(a) Information of Data Subjects ... 8
(b) Easy access to BCR ... 8
16. Task of DPO ... **8**
17. Right to lodge a complaint ... **9**
18. Internal complaint handling procedures ... **9**
19. Third party Beneficiary rights ... **10**
20. Process for updating the BCR ... **10**
21. Notification and Documentation of Data Breaches ... **11**
22. Training Programme ... **11**
23. Monitoring/Audit Programme ... **11**
24. Cooperation with Supervisory Authorities ... **12**
25. Non-Compliance with these BCR ... **12**
26. Effective Date ... **13**
27. Annexes ... **13**

Annex 1 ..... **14**
Annex 2 ..... **15**
Annex 3 ..... **17**
Annex 4 ..... **20**

1. Introduction

The Munich Re Group is dedicated to establish a single set of global rules to ensure an adequate protection of Personal Data Processed within Munich Re Group worldwide. As part of this commitment to a high level of privacy, Munich Re Group has enacted these Binding Corporate Rules (in the following "BCR") in order to provide for appropriate safeguards and guarantees ensuring an Adequate Level of Data Protection in accordance with the GDPR (Regulation (EU) 2016/679) for any Transfer, including the subsequent Processing, of EEA Data by or on behalf of Munich Re Group Members within the EEA to Munich Re Group Members in Third Countries.

These BCR are binding for all Munich Re Group Members including the Reinsurance Group (with GSI members), ERGO Group and MEAG Group and must be respected by the employees of the whole Munich Re Group. Given the essential role of these BCR for the protection of Personal Data within Munich Re Group, the Board of Management of Munich Re Munich is committed to ensure an effective implementation of and compliance with the BCR within Munich Re Group.

2. Scope of the Binding Corporate Rules

These BCR shall apply to the Transfer, including the subsequent Processing, of EEA Data by or on behalf of Munich Re Group Members within the EEA to Munich Re Group Members in Third Countries. **Annex 1** lists all Munich Re Group Members in their role as Data Controllers (including, as the case may be, as Data Processors for other Munich Re Group Members).

A description of the Processing operations and Data Transfers within the Munich Re Group under the scope of these BCR is contained in **Annex 2**.

3. Definitions and References

The terms and expressions used in these BCR with capital letters shall have the meaning as defined in **Annex 3**.

Annex 4 includes the wording of the GDPR Articles referenced in these BCR. Any reference to requirements set forth in the Articles enlisted in these BCR is made in order to mirror such content and should be understood as a commitment undertaken by all Munich Re Group Members to put in place the same level of safeguards as set forth in those Articles.

4. General Data protection principles

The general data protection principles as stipulated in Article 5 of the GDPR apply to these BCR, in particular the principles of purpose limitation, data minimisation, storage limitation, accuracy, integrity and confidentiality. Further Munich Re Group Members undertake to process EEA Data lawfully, fairly and in a transparent manner in relation to the Data Subject.

Additionally the principles of data protection by design and by default, legal basis for processing, processing of Sensitive Data and the requirements in respect of onward transfers to bodies not bound by these BCR as described in more detail in the following Sections (5, 6, 7, 12) shall also apply to these BCR.

5. Legal basis for Processing of EEA Data

EEA Data shall only be Processed based on suitable grounds of lawfulness as those stipulated especially in Article 6 para 1 of the GDPR, in particular where (i) the Data Subject has given consent, (ii) processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, (iii) processing is necessary for entering into or performance of a contract to which the Data Subject is party or (iv) processing is necessary

for compliance with a legal obligation laid down by European Union (EU) or EU Member State law.

6. Legal basis for Processing of Sensitive EEA Data

Munich Re Group Members in Third Countries undertake not to Process Sensitive EEA Data if there is no ground of lawfulness. Suitable grounds of lawfulness as those stipulated especially in Article 9 para 2 of the GDPR are in particular where (i) the Data Subject has given explicit consent, (ii) processing is necessary for the establishment, exercise or defence of legal claims or (iii) processing is necessary for reasons of substantial public interests.

Munich Re Group Members recognize that the Processing of EEA Data relating to criminal convictions and criminal offenses is prohibited unless it is carried out under the control of an official authority or it is permitted under applicable EU or EU Member State law that provides appropriate safeguards for the rights and freedoms of data subjects.

7. Accountability

Every Munich Re Group Member as Data Controller shall be responsible for and able to demonstrate compliance with these BCR.

For this reason, all Munich Re Group Members maintain a record of all Processing activities regarding EEA Data containing all elements set forth in Article 30 para 1 (in their role as Data Controllers) and Article 30 para. 2 of the GDPR (in their role as Data Processors). This record will be maintained in writing, including in electronic form, and will be made available to the Competent Supervisory Authority on request.

In order to enhance compliance and when required, data protection impact assessments in line with the requirements set forth in Article 35 para 1 of the GDPR will be carried out for Processing operations for EEA Data that are likely to result in a high risk to the rights and freedoms of natural persons. Where such data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk, the Competent Supervisory Authority, prior to Processing, will be consulted in line with the requirements set forth in Article 36 para 1 of the GDPR.

All Munich Re Group Members have implemented, and undertake to maintain, appropriate technical and organisational measures to implement data protection principles and to facilitate compliance with the requirements set up by these BCR in practice (Data Protection by Design and by Default).

8. Rights of Data Subjects

In regard to Processing EEA Data the Data Subject has the same rights as those recognized in Articles 12 to 19 and 21 to 22 of the GDPR, in particular the right of information, access, rectification, erasure, restriction of processing as well as the right to object and not to be subject to decisions based solely on automated Processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This applies subject to restrictions laid down by European Union (EU) or EU Member State law applicable to the Data Exporter.

Data Subjects can exercise their above rights by contacting the Data Protection Function competent for the respective Munich Re Group Member acting as Data Controller with respect to their EEA Data. Contact details of the competent Data Protection Function for each Munich Re Group Member are published on the public internet website of Munich Re Reinsurance Group.

Additionally, the Data subject has the right to complain through the internal complaint handling procedures set out in Section 18.

9. Data security

All Munich Re Group Members have implemented, and undertake to maintain, appropriate technical and organisational measures to protect EEA Data against unlawful forms of Processing. In particular these measures shall protect EEA Data against unauthorized Processing, alteration, loss, accidental destruction or damage, unauthorized disclosure of, or access to EEA Data transmitted, stored or otherwise Processed (integrity and confidentiality).

Such measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the EEA Data. Sensitive Data shall be Processed with enhanced security measures.

10. Third Country laws and practices assessment

Munich Re Group Members undertake to use these BCR as a tool for a Transfer only if they have assessed and no reason to believe that the laws and practices in the Third Country of destination applicable to the Data Importer when Processing EEA Data, including any requirements for disclosure of EEA Data or measures authorizing access by public authorities, prevent the Data Importer from complying with its obligations under these BCR.

This is based on the understanding that laws and practices, that respect the essence of fundamental rights and freedoms and do not go beyond what is necessary and proportionate in a democratic society to protect an overriding objective listed in Article 23 para. 1 of the GDPR are not in contradiction with these BCR. In assessing the laws and practices of the Third Country that may affect compliance with the obligations set forth in these BCR, Munich Re Group Members shall take into account, in particular:

- The particular circumstances of the Transfer(s) and any intended onward Transfer within the Third Country or to another Third Country, including:
    - the purpose for which the EEA Data is Transferred and Processed
    - the types of entities involved in the Processing
    - the economic sector(s) in which the Transfer(s) will take place
    - the categories and format of the EEA Data Transferred
    - the place where the Processing of the EEA Data takes place, including its storage
    - the channels used for the Transfer

- The laws and practices of the Third Country of destination relevant in the light of the specific circumstances of the Transfer(s), including those laws and practices requiring disclosure of EEA Data to, or permitting access by public authorities and those providing for access to such EEA Data during the Transfer between the country of the Data Exporter and the country of the Data Importer and the limitations and safeguards applicable thereto.

- Any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these BCR, including the measures applied during the Transfer and processing of the EEA Data in the Third Country of destination.

The Group Data Protection Officer will be informed and involved in such assessment. The assessment, as well as the additional measures selected and implemented, will be documented by the Munich Re Group Members and made available to the other Munich Re Group Members as well as, upon request, to the Competent Supervisory Authority. The assessment is continuously reviewed for developments that may affect the original assessment.

In case a Munich Re Group Member, in its role as Data Importer, has reason to believe that applicable Third country laws or practices might prevent it from fulfilling its obligations under these BCR, including following a change in the laws in the Third Country or a measure, it shall promptly inform the Data Exporter and the Group Data Protection Officer thereof.

Upon review of such information, or if it otherwise has reason to believe that the Data Importer can no longer comply with its obligations under these BCR, the Data Exporter and the Group Data Protection Officer, shall promptly identify additional measures to be taken by the Data Exporter and/or the Data Importer to enable the respective Munich Re Group Member to comply with its obligations under these BCR. The same applies if a Data Exporter has reasons to believe that the Data Importer can no longer fulfil its obligations under these Binding Corporate Rules. The Group Data Protection Officer shall inform all other Munich Re Group Members of the result of the review so that the result of the review can be adopted in the case of comparable transfers.

11. Third Country government access requests

(a) Notification

The Data Importer will promptly notify the Data Exporter, the Group Data Protection Officer and, if feasible (with the assistance of the Data Exporter), the Data Subject if it:

- receives a request for information from an authority in the Third Country that is legally binding under the law of the country of destination or another Third Country and that concerns EEA Data Transferred under these BCR. The notification shall contain information about the EEA Data requested, the authority requesting the information, the legal basis for this request, and the response given to the request.

- becomes aware that an authority in the Third Country has direct access to EEA data transferred under these BCR in accordance with the law of the country of destination. The notification shall include all information available to the Data Importer.

If the Data Importer is prohibited from notifying the Data Exporter and/or the Data Subject, the Data Importer shall use its best efforts to obtain a waiver of such prohibition in order to provide as much information as possible and as soon as possible. These efforts shall be documented in order to be able to demonstrate them to the Data Exporter upon request.

The Data Importer shall provide the Data Exporter with as much information as possible on requests for information received at regular intervals. Should the Data Importer be (partially) prohibited from doing so, it shall, without undue delay, inform the Data Exporter of this prohibition under the laws of the country of destination. The Data Importer shall retain this information for as long as the EEA Data is subject to the safeguards of these BCR. It shall be made available to the Competent Supervisory Authority upon request.

(b) Review of legality and data minimisation

The Data Importer shall review the legality of the request for information, in particular whether it is within the powers granted to the requesting public authority. It shall challenge the request if, after careful consideration, it concludes that there are reasonable grounds to believe that the request is unlawful under the laws of the country of destination, applicable obligations under international law and the principles of international comity. The Data Importer will appeal under the same conditions. When challenging a request for information, the Data Importer shall apply for interim measures with the aim of suspending the effects of the request for information until the competent judicial authority has ruled on the legality of the request for information. It shall not release the requested personal data until it is obliged to do so under the applicable procedural rules.

The Data Importer shall document its legal assessment and any challenges to the request for information. To the extent permitted by the law of the country of destination, it shall make this documentation available to the Data Exporter and the Group Data Protection Officer. Upon request, the Data Importer shall make the documentation available to the Competent Supervisory Authority.

When responding to a request for information, the Data Importer shall provide the minimum permissible amount of information as determined by a reasonable interpretation of the request for information.

In case a Munich Re Group Member, in its role as Data Importer, has reason to believe that Transfers of EEA Data to a public authority in a Third Country can be massive, disproportionate and indiscriminate in a way that goes beyond what is necessary in a democratic society, Section 10 shall apply.

12. Relationships with Data Processors

Where EEA Data is to be Processed on behalf of a Munich Re Group Member it undertakes to enter into contracts with all internal and external subcontractors/processors. The contracts shall comprise the same requirements as those envisaged by Article 28 para. 3 of the GDPR.

13. Restriction on Transfers and onward Transfers outside the Munich Re Group to and in Third Countries

If a Munich Re Group Member intends to Transfer EEA Data to an External Data Controller or Data Processor located in a Third Country not providing an Adequate Level of Data Protection, it undertakes to take appropriate safeguards to comply with the same requirements as those envisaged by Articles 45, 46 and 49 of the GDPR.

14. Liability

Every Munich Re Group Member exporting EEA Data to a Third Country on the basis of these BCR (i) accepts responsibility for and agrees to take the necessary action to remedy the acts of a Munich Re Group Member in a Third Country bound by the BCRs for which it is the Data Exporter and (ii) shall be liable to Data Subjects for any breaches of these BCR by such a Munich Re Group Member established in a Third Country which received the data from this Munich Re Group Member. The exporting Munich Re Group Member shall be entitled to claim reimbursement of any compensation paid for a breach from the receiving Munich Re Group Member corresponding to the receiving Munich Re Group Member’s part of responsibility for the breach.

If a Munich Re Group Member exporting EEA Data can prove that the receiving Munich Re Group Member in a Third Country is not responsible for the event giving rise to the damage, or that no breach of these BCR took place, it may discharge itself from any responsibility and liability. The receiving Munich Re Group Member in the Third Country undertakes to reasonably cooperate and assist the exporting Munich Re Group Member.

If a Munich Re Group Member established in a Third Country violates these BCR, the courts or other competent authorities in the EU will have jurisdiction and the data subject will have the rights and remedies against the exporting Munich Re Group Member that has accepted responsibility and liability as if the violation had been caused by them in the Member State in which they are based instead of the Munich Re Group Member.

15. Transparency and easy access to BCR for Data Subjects

(a) Information of Data Subjects

All Data Subjects benefitting from the third party beneficiary rights shall in particular be provided with the same information as those referred to in Articles 13 and 14 of the GDPR, information on their third party beneficiary rights with regard to the processing of their EEA Data and on the means to exercise those rights. Further the Data Subjects shall be provided with the information on the scope of these BCR (Section 2), the data protection principles (Section 4), the lawfulness of the processing (Sections 5 and 6), the rights of the Data Subjects (Section 8), the data security (Section 9), the personal data breach notifications (Section 21 para. 3), the restrictions on onward Transfers (Section 13) and the liability (Section 14). The information shall be complete and not only summarized.

(b) Easy access to BCR

The relevant parts of these BCR (including, in particular, Section 18 and those other provisions of these BCR covered by the Data Subject's third party beneficiary rights, and the list of Munich Re Group Members bound by these BCR) are, and shall continue to be, published on the public internet website of Munich Re Reinsurance Group to inform Data Subjects about their rights. In addition, Data Subjects shall be provided with a copy of the relevant parts of these BCR upon request to the competent Data Protection Function or to the Group Data Protection Officer.

16. Task of DPO

Munich Re Group has appointed, and shall continue to ensure the appointment of, appropriate staff with the highest management support to oversee and monitor compliance with these BCR.

The Group Data Protection Officer is appointed by Munich Re Munich and works to monitor compliance with these BCR. The Group Data Protection Officer advises and directly reports to the Board of Management of Munich Re Munich and should have no tasks that could result in conflict of interests.

The Group Data Protection Officer

- decides where a Data Protection Function will be appointed for one or more specific Munich Re Group Member(s) at the company or regional level.
- deals, when necessary, with the help of Data Protection Functions, with investigations by Supervisory Authorities related to the BCR.
- monitors and annually reports on compliance with these BCR at a global level whereas the Data Protection Functions support him/her in these regards on a local level.

The Data Protection Functions

- shall support the Group Data Protection Officer in the endeavour to ensure implementation of and compliance with these BCR.
- shall have a technical reporting line to the Group Data Protection Officer.
- will report major privacy issues relating to the BCR to the Group Data Protection Officer and will provide advice, monitor training and compliance as regards to these BCR at a local level.

- as stipulated in Section 18, can be in charge, were appropriate, of handling local complaints from Data Subjects as to the processing under these BCR.

- as stipulated in Section 23, perform regular reviews of the data processing systems and applications at the respective Munich Re Group Member for their compliance with legal and internal data privacy requirements of the BCRs. Additionally, the Group Data Protection Officer can request audits to be conducted by Data Protection Functions at any time.

The Group Data Protection Officer can further specify the above tasks of the Data Protection Functions.

The Group Data Protection Officer and the Data Protection Functions can be directly contacted, for which contact details are published on the public internet website of Munich Re Reinsurance Group.

17. Right to lodge a complaint

The Data Subject has the right to lodge a complaint to enforce any of the data subject's third party beneficiary rights. The claim could be brought either before a Supervisory Authority, in particular before the Competent Supervisory Authority in the EU Member State of his or her habitual residence, place of work or place of the alleged infringement. Or the claim could also be brought before the competent courts of the EU Member States within the jurisdiction of the Data Exporter or before the court competent for Munich Re Munich, or where the Data Subject has his or her habitual residence (as a choice for the Data Subject).In this regard, the Data Subject may be represented by a not-for-profit body, organisation or association duly constituted under the law of a Member State of the European Union, whose statutory objectives are in the public interest and which is active in the field of the protection of the rights and freedoms of data subjects with regard to the protection of their Personal Data.

18. Internal complaint handling procedures

Munich Re Group has put in place, and undertakes to maintain, an internal complaint handling system that allows any Data Subject to complain that any Munich Re Group Member is not complying with these BCR.

For this purpose, the relevant details of the complaint handling procedure and the necessary contact information for filing complaints (email and postal address) are part of Annex 1 and published on the public internet website of Munich Re Reinsurance Group.

Munich Re Reinsurance Group undertakes to ensure that for each Munich Re Group Member the nominated Data Protection Function will be competent for handling complaints relating to such Munich Re Group Member. If more than one Munich Re Group Member is involved in a complaint, the complaint shall be forwarded to the Group Data Protection Officer.

Munich Re Group undertakes to ensure that the Data Protection Function competent for handling the complaints benefit from an appropriate level of independence in the exercise of his/her functions.

Data Subjects may file a complaint regarding compliance with these BCR electronically via the contact form on the public internet website of Munich Re Group or by postal letter. Complaints shall be handled in accordance with the following procedure.

The competent Data Protection Function shall initiate an appropriate investigation within the concerned Munich Re Group Member. All complaints shall be dealt with, without undue delay and in any event within one month. Taking into account the complexity and/or number of the

complaints, that one month period may be extended at maximum by two further months, in which case the Data Subject will be informed accordingly.

If the findings of the investigation reveal that the complaint is justified, the Data Protection Function will cooperate with the Managing Director of the concerned Munich Re Group Member and the Group Data Protection Officer as appropriate, to monitor the implementation of the relevant measures to resolve the complaint. The Data Protection Function may advise the departments on the appropriate measures to achieve compliance with the corporate guidelines and any applicable data privacy laws. The Data Protection Function informs the Data Subject of the findings of the investigation and the corresponding remediation measures, as well as the option to escalate the complaint to the Group Data Protection Officer if he/she is not satisfied by the result or handling of his/her complaint.

If the findings of the investigation reveal that the complaint is not justified, the Data Protection Function will inform the Data Subject of the findings and of the option to escalate the complaint to the Group Data Protection Officer if he/she wishes to challenge such findings.

In all cases, the Data Protection Function will inform the Data Subject, together with the findings of the investigation, of his/her right to file a complaint or to lodge a claim before the competent court according to Section 17.

19. Third party Beneficiary rights

The Data Subject shall have the right to enforce Sections 4, 5, 6, 8, 9, 10, 11, 13, 14, 15, 17, 18, 20 para. 4 (ii), 21 para. 3 and 24 (relating to compliance obligations covered by this third party beneficiary clause) of these BCR as third party beneficiary, and provided that the Data Subject's claim relates to EEA Data.

The third party beneficiary rights shall include judicial remedies for any breach of the rights guaranteed and the right to receive compensation.

20. Process for updating the BCR

These BCR may be updated and/or modified in accordance with applicable internal norms of the Munich Re Group, for instance where necessary to take into account modifications in the regulatory environment or of the Data Processing operations within Munich Re Group.

Any updates to the list of Munich Re Group Members bound under these BCR (as necessary to reflect changes to the Munich Re Group structure and/or to include new entities to the group of Munich Re Group Members bound under these BCR after the Effective Date) may be made in accordance with applicable internal norms of Munich Re Group by updating **Annex 1** of these BCR.

Munich Re Group undertakes to report any changes of these BCR as well as any updates to the list of Munich Re Group Members contained in **Annex 1**, to the Competent Supervisory Authorities via the Lead Supervisory Authority at least once a year with a brief explanation of the reasons for the update. Where a modification would possibly affect the level of the protection offered by these BCR or significantly affect these BCR (i.e. changes to the binding character), it must be communicated in advance to this Supervisory Authority. The Lead Supervisory Authority shall also be notified once a year in instances where no changes have been made.

Any updates or modifications to these BCR or its Annexes shall be communicated to (i) Munich Re Group Members by publishing a revised version of these BCR or, as applicable, an updated version of **Annex 1** in Munich Re Reinsurance Group's intranet, ERGO Group’s intranet and MEAG Group’s intranet in accordance with internal norms of the Munich Re Group without undue

delay and (ii) to data subjects by publishing relevant parts of the revised versions of these BCR on the public internet website of Munich Re Reinsurance Group as stipulated in Section 15 (b).

The Group Data Protection Officer is responsible to keep track of and record any updates to these BCR and to maintain a fully updated list of the Munich Re Group Members bound by these BCR, including their respective effective date of inclusion under these BCR. The respective Munich Re Group Member shall inform the Group Data Protection Officer without undue delay on any updates. The Group Data Protection Officer shall provide the necessary information to the Data Subjects or the Competent Supervisory Authority upon request.

In case a new member shall be included to the Munich Re Group Members bound under these BCR after the Effective Date, no Transfer of EEA Data may be made to the new member under these BCR until such member is effectively bound by these BCR and can deliver compliance with these BCR.

21. Notification and Documentation of Data Breaches

In case of any EEA Data Breach, the respective Munich Re Group Member which acted as a Data Importer shall notify without undue delay the EEA Data breach to the Data Exporter and its Data Protection Function. This also applies if the respective Munich Re Group Member is the Data Processor and the Data Exporter acts as the Data Controller.

In case of an EEA Data Breach, the respective Munich Re Group Member as the Data Controller must notify the Competent Data Protection Authority without undue delay and, if possible, within 72 hours of becoming aware of the EEA Data Breach, unless the EEA Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

In case of any EEA Data Breach, which is likely to result in a high risk to the rights and freedoms of natural persons, the respective Munich Re Group Member shall notify the EEA Data breach to the Data Subject without undue delay.

Any EEA Data breaches should be documented (comprising the facts relating to the EEA Data breach, its effects and the remedial action taken). This documentation shall enable the Competent Supervisory Authority to verify compliance with the GDPR. The documentation should be made available to the Competent Supervisory Authority on request.

22. Training Programme

Munich Re Group has implemented, and undertakes to maintain, a data protection training programme for all personnel who have permanent or regular access to EEA Data during the performance of their work and/or are involved in the collection of EEA Data or in the development of tools used to Process EEA Data. The training programme will be updated regularly as needed and covers, among others, procedures of managing requests for access to EEA Data by public authorities in Third Countries. The personnel concerned are required to perform a training at least every three years.

23. Monitoring/Audit Programme

The Data Protection Function performs regular monitoring measures of the data processing systems and applications at the respective Munich Re Group Member for their compliance with legal and internal data privacy requirements of the BCRs. Additionally, the Group Data Protection Officer can request monitoring measures to be conducted by Data Protection Functions at any time.

Furthermore, Munich Re Group has implemented, and undertakes to maintain, an audit programme verifying compliance with these BCR on a regular basis and if there are indications

of non-compliance. The audit programme covers all aspects of these BCR including methods and action plans ensuring that corrective actions to protect Data Subject rights will take place.

Regular data privacy audits which encompass compliance with these BCR at the Munich Re Group Members are conducted at recurring intervals at least every five years based on a risk-oriented audit-programme. Regular data privacy audits are conducted by internal (Group Audit) or external accredited auditors. The audit plan is determined in the regional audit hubs, approved by the legal entity audit committees and/or boards of management (if appropriate) and conducted by the responsible team within Group Audit. To ensure Group adherence to these BCR the regional audits plans, in respect of data privacy audits, are overseen centrally by the Europe & Latin America Regional Hub. The global audit plan is notified to the Board of Management of Munich Re Munich on a quarterly basis. If audits are carried out by external auditors, these auditors should have appropriate experience in carrying out such audits on the basis of the GDPR and can demonstrate corresponding expertise. Furthermore, the Group Data Protection Officer can request for the conducting of additional data privacy audits by external auditors.

The results of an audit will be communicated to the Group Data Protection Officer, to the Managing Director of the respective Munich Re Group Member and the responsible member of the Board of Management of Munich Re Munich. Competent Supervisory Authorities can receive a copy of such audit reports upon request. Such audit reports may contain confidential information subject to a duty of professional secrecy for the member or members and the staff of the Supervisory Authority (e.g., as set forth in Article 54 para 2 of the GDPR), and may be protected as business secrets under applicable freedom of information laws.

Each Munich Re Group Member accepts that they could be audited by the Competent Supervisory Authority and that they will abide by the Decisions of the Supervisory Authorities on any issue related to these BCR. This is without prejudice to any right to appeal any Decision of the Supervisory Authorities.

24. Cooperation with Supervisory Authorities

The Munich Re Group Members undertake to reasonably cooperate and assist each other to ensure compliance with these BCR and to handle a request or complaint from a Data Subject or an investigation or inquiry by the Competent Supervisory Authority. The Munich Re Group Members shall provide the Competent Supervisory Authority, upon request, with all information on the processing operations covered by these BCR.

The Munich Re Group Members further agree to cooperate with, to and to abide by the Decisions of this Supervisory Authority on any issues regarding the interpretation of these BCR. This is without prejudice to any right to appeal any Decision of the Supervisory Authorities. The Munich Re Group Members acknowledge that the courts of the EU Member State where the Competent Supervisory authority is located are responsible for this in accordance with their respective procedural law and the Munich Re Group Members undertake to submit themselves to the jurisdiction of these courts.

25. Non-Compliance with these BCR

If a Data Importer is unable to comply with these BCR for any reason, it shall immediately inform the Data Exporter thereof.

Upon review of such information, or if the Data Exporter otherwise has knowledge that the Data Importer is unable to comply with these BCR or is in breach of these BCR, the Data Exporter shall suspend the transfer of personal data to the Data Importer until compliance with these BCR is again ensured.

The Data Importer shall, at the choice of the Data Exporter, immediately return or delete the EEA Data that has been transferred under the BCR in its entirety including any copies, where:

- the Data Exporter has suspended the transfer, and compliance with these BCR is not restored within a reasonable time, and in any event within one month of suspension; or
- the Data Importer is in substantial or persistent breach of these BCR; or
- the Data Importer fails to comply with a binding decision of a competent court or the Competent Supervisory Authority regarding its obligations under these BCR

If the Data Exporter choses the deletion of the EEA Data, the Data Importer shall certify the deletion to the Data Exporter. Until the EEA Data has been deleted or returned, compliance with these BCR shall be ensured.

In case of Third Country laws applicable to the data importer that prohibit the return or deletion of the transferred EEA Data, the Data Importer should warrant that it will continue to ensure compliance with these BCR, and will only process the data to the extent and for as long as required under that Third Country law.

Section 10 remains unaffected insofar as Third Country laws and/or practices affect compliance with these BCR.

26. Effective Date

These BCR enter into force as of 1 January 2024 ("**Effective Date**").

Any updates or modifications to these BCR, including its **Annexes**, shall enter into force on the date of the publication of a revised version of these BCR (containing the corresponding updates or modifications) on the public internet website of Munich Re Reinsurance Group in accordance with internal norms of the Munich Re Group. The revised version of these BCR shall state its Effective Date

Where a non-EEA Munich Re Group Member ceases to be part of the Munich Re Group or to be bound by the BCR in the future, it will continue to apply the BCR requirements to the Processing of the EEA Data Transferred to it by means of the BCR unless, at the time of leaving the Munich Re Group, it will delete or return the entire amount of the EEA Data to Munich Re Group Members to which the BCRs still apply.

27. Annexes

These BCR include the following Annexes:

Annex°1: List of Munich Re Group Members bound by the Binding Corporate Rules

Annex°2: Description of Processing operations and Data Transfer

Annex°3: Definitions

Annex°4: Wording of the GDPR Articles referenced in these BCR

Annex 1

List of Munich Re Group Members bound by the Binding Corporate Rules

The list of Munich Re Group Members bound by the BCR can be accessed at any time under the Privacy tab on the public internet website of Munich Re Reinsurance Group and the list shows the structure and the contact details of all the Munich Re Group Members, including their addresses, company registration numbers and the point(s) of contact where data subjects can lodge any complaints related to the processing of their personal data covered by the BCR.

Annex 2

Description of Processing operations and Data Transfer

In particular this Annex shall show the Nature of EEA Data, the Categories of Data Processed, the Purposes and the Transfer of the Data.

1. Scope

These BCR of the Munich Re Group cover the Processing by or on behalf of Munich Re Group Members in their role as Data Controllers or Data Processors of EEA Data relating to:

- current, former or prospective representatives and employees of Munich Re Group Members, including but not limited to, full time, part time, interim and casual workers, contractors and temporary workers, applicants, interns, student trainees, retirees and relations of employees ("**HR Data**")

- representatives, employees and contact persons at current, former or prospective corporate customers, including but not limited to, brokers, agents, intermediaries, banks, experts suppliers, service providers or other business partners of Munich Re Group Members ("**Business Partner Data**")

- current, former or prospective customers of primary insurers/cedents, including but not limited to, clients, policyholders claimants, beneficiaries, physicians and other experts ("**(Re-) Insurance Data**")

2. Nature of the Data and Categories of EEA Data Processed

The Nature of the EEA Data is as follows:

- **HR Data**, including, but not limited to, basic details (e.g. name, title, business contact details, positions), CV data (e.g. age and date of birth, private address, marital status, religion, education, professional experience, skills, hobbies, languages), employment contracts and financial data (e.g. bank account and salary information), health and absence data (e.g. reason for absence, disability), performance details (e.g. appraisals, ratings, disciplinary actions), IT related employee data (e.g. logfiles, user ID, access rights, employee number), employee travel and expenses information (e.g. bookings, passport and visa details), background checks (e.g. relevant criminal convictions, proof of eligibility to work), photos and videos (e.g. photo in group's global contact data base)

- **Business Partner Data**, including, but not limited to, basic details (e.g.name, title, business contact data), business activities (e.g. goods or services provided; in the context of compliance questionnaires also names of shareholders and representatives, data regarding legal proceedings, relationships with office holders, bank account details, references, to the extent lawful under applicable EU or EU Member State law health data

- **(Re-)Insurance Data**, including but not limited to, insurance contract data (e.g. name, date of birth, sum insured from the application, commencement and term of the insurance contract), data relating to a damage event, health data (e.g. details of physical or psychological health, medical condition), data regarding legal proceedings

- HR Data, Business Partner Data and (Re-)Insurance Data may contain limited categories of Sensitive Data where strictly necessary for the respective purpose of Processing

3. Purposes of the Processing and transfers

EEA Data shall be Processed only as necessary for one or more of the following specified purposes or as required by applicable EU or EU Member State law. EEA Data will only be Transferred and/or made accessible on a need-to-know basis and to the extent necessary for the relevant purpose. The EEA Data will be transmitted from Munich Re Group Members within the EEA to Munich Re Group Members in countries outside the EEA. EEA Data is Processed and Transferred by Munich Re Group Members in particular for the following purposes:

- **HR Data**: human resources management and group internal administrative purposes including, but not limited to, general administration of the employment relationship (e.g. payroll), employee management in Munich Re Group's matrix structure, global collaboration, training programmes, employee performance and career development, workforce and succession planning and talent management, global mobility of employees (e.g. assignments to Munich Re Group Members), IT support services management, internal support activities management (e.g., legal; internal audit), security and business continuity management (e.g. continuity and crisis planning and response); compliance with legal obligations (e.g. whistleblowing)

- **Business Partner Data**: partner relationship management and administration including, but not limited to, preparing for creating and performing contractual relationships, enabling global collaborations on business partner projects and providing business partner service and support, and for the purpose of ensuring compliance with legal requirements, preparation/implementation and termination of (re-)insurance agreements in all classes of insurance, centralized customer relationship management ("CRM") database

- **(Re-)Insurance Data**: insurance and reinsurance purposes including, but not limited to, entering into and performance of (re-)insurance agreements (e.g. carry out a risk assessment), internal administrative purposes (e.g. group-wide reinsurance accumulation control) and group internal support and services (e.g. centers of competence), statistical analysis and compliance with legal obligations (e.g. sanction lists)

Annex 3

Definitions

The terms and expressions used in these Binding Corporate Rules with capital letters shall have the following meaning:

“**Adequate Level of Data Protection**” means the level of data protection deemed "adequate" under Article 45 of the GDPR, as provided for in the following countries: 1) all EU Member States, 2) Iceland, Liechtenstein and Norway, 3) countries for which the European Commission has issued an adequacy decision (currently Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom and Uruguay) and/or 4) all countries that may join the European Union and/or about which a decision regarding adequacy will be issued by the European Commission.

"**BCR**" means these Munich Re Binding Corporate Rules for the Processing of Personal Data by Munich Re Group Members.

“**Board of Management of Munich Re Munich**” means the Board of Management of Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München, Munich.

„**Competent Supervisory Authority**“ for EEA Data means the Supervisory Authority that is competent pursuant to Articles 55, 56 of the GDPR for the Data Exporter.

“**Data 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.

“Data Breach” means means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

“**Data Exporter**” means a Munich Re Group Member operating as Data Controller in the EEA, that Transfers Personal Data out of the EEA to another Munich Re Group Member based in a country that does not provide an Adequate Level of Data Protection.

“**Data Importer**” means a Munich Re Group Member operating as Data Controller or Data Processor in a Third Country, which receives Personal Data out of the EEA from another Munich Re Group Member based in the EEA.

“**Data Processor**” means the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

“**Data Protection Function**” means any data protection officer locally appointed for one or more specific Munich Re Group Member(s). If no data protection officer is appointed for a Munich Re Group Member it means the local representative (natural person) appointed as Data Protection Expert for one or more specific Munich Re Group Member(s) at the company or regional level or segment level and in charge of providing advice for an adequate protection of Personal Data and monitoring compliance with these BCR and applicable law on local level for such Munich Re Group Member.

“**Data Subject**” means an identified or identifiable natural person to whom the Personal Data Processed by or on behalf a Munich Re Group Member relate.

“**Decisions**” mean any formal decision from a Supervisory Authority with legal effect provided the decision is not subject to a suspensory effect from legal proceedings at the competent courts within the EU, and without limiting the right to appeal such formal decision in accordance with the applicable EU or EU Member State laws for the Supervisory Authority.

“**EEA**” means all Member States of the European Union, plus Iceland, Lichtenstein and Norway.

“**EEA Data**” means any Personal Data that are or have been Processed by or on behalf of a Munich Re Group Member within the EEA in its role as Data Controller and thereby are or have been subject to the GDPR.

“**Effective Date**” means the date on which these Binding Corporate Rules become effective as set forth in Section 26.

„**ERGO**“ means ERGO Group AG with registered seat at ERGO-Platz 1, 40198 Düsseldorf, Germany, the ultimate parent company of the ERGO Group.

“**ERGO Group**”, means ERGO and all entities wholly or partially owned by ERGO including their branches and representative offices.

"**GDPR**" means the 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.

“**Group Data Protection Officer**” means the representative (natural person) appointed as such at Munich Re Munich and in charge of providing advice for an adequate protection of Personal Data and monitoring compliance with these BCR on a group-wide level with respect to any Processing within the Munich Re Group.

“**GSI**” means Global Specialty Insurance, i.e. Munich Re Reinsurance Group members writing specialty primary insurance business or performing services which are booked under Munich Re Munich's reinsurance segment.

„**Lead Supervisory Authority**“ means the Supervisory Authority that is competent to act as BCR lead supervisory authority pursuant to the Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors (wp263rev.01) endorsed by the European Data Protection Board, i.e. the Data Protection Authority of Bavaria for the Private Sector.

“**Managing Director**” means the Chief Executive Officer, General Manager or any other executive head of the concerned Munich Re Group Member

„**MEAG**“ means MEAG MUNICH ERGO Asset Management GmbH with registered seat at Am Münchner Tor 1, 80805 Munich, Germany, the ultimate parent company of the MEAG Group.

“**MEAG Group**”, means MEAG and all entities wholly or partially owned by MEAG including their branches and representative offices.

“**Munich Re Munich**”, Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München with registered seat at Königinstraße 107, 80802 Munich, Germany, the ultimate parent company of Munich Re Group.

“**Munich Re Group**” means Munich Re Munich, ERGO Group, MEAG Group and all other legal entities wholly or partially owned by Munich Re Munich, including their respective branches and representative offices, excluding.

“**Munich Re Group Member**” means all members of the Munich Re Group who signed the Intra Group Agreement as set forth in Attachment 2 of the Guideline on Binding Corporate Rules to the extent listed in **Annex 1**.

“**Personal Data**” means any information relating to an identified or identifiable natural person (the Data Subject); an identifiable 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.

“**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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“**Sensitive Data**” means any 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.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to Article 51 GDPR (please find the wording of this Article in Annex 4).

"**Third Country**" means a country which does not have an Adequate Level of Data Protection.

“**Transfer**” means any disclosure of EEA Data, including by transmission, dissemination or otherwise making available to a recipient.

Annex 4

Wording of the GDPR Articles referenced in these BCR

The wording of the GDPR Articles referenced in these BCR reads as follows:

Article 5 Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) 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) [1], not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6 Lawfulness of processing

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;

[1] Art. 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 the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

(b) processing is necessary for the performance of a contract 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 contract;

(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;

(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.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10[2];

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 9 Processing of special categories of personal data

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.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or

[2] Art. 10: Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

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[3] 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.

[3] Art. 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.

(2) The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

(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.

(4) If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2) [4], the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

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.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions 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 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 shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Article 13 Information to be provided where personal data are collected from the data subject

[4] Art. 11 (2): Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

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 contact details of the controller and, where applicable, of the controller's representative;

(b) the contact 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 fact 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 contractual requirement, or a requirement necessary to enter into a contract, 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.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall 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 paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14 Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact 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) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in 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[5], or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means 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 provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(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) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) 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 and to object to processing as well as the right to data portability;

(d) where 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;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) 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.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

[5] Art. 47 Binding Corporate Rules

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall 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 paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(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.

Article 15 Right of access by the data subject

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;

(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.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall 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 shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Article 16 Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

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

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).

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.

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

(e) for the establishment, exercise or defence of legal claims.

Article 18 Right to restriction of processing

1. The data subject shall have 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 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.

2. Where processing has been restricted under paragraph 1, such personal data shall, 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 of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 21 Right to object

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.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. 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.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22 Automated individual decision-making, including profiling

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.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Article 23 Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in

Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) 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 public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. (…)

Article 28 Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act 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. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32[6];

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36[7] taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

[6] Art. 32 Security of processing

[7] Art. 34 Communication of a personal data breach to the data subject

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 30 Records of processing activities

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

(a) the name and contact 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;

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

2. Each processor and, where applicable, the processor's representative shall 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, 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;

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

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

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.

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.

Article 35 Data protection impact assessment

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.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

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.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

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.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36 Prior consultation

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.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the

performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Article 45 Transfers on the basis of an adequacy decision

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.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2) [8].

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a

[8] Art. 93: 1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011 .

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011 , in conjunction with Article 5 thereof, shall apply.

third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46 Transfers subject to appropriate safeguards

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;

(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[9] 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[10] 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.

[9] Art. 40 Codes of Conduct

[10] Art. 42 Certification

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) contractual 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.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63[11] in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 49 Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with

[11] Art. 63 Consistency mechanism

regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 51 Supervisory authority

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').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 55 Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56 Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61[12] and 62[13].

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

[12] Art. 61 Mutual assistance

[13] Joint operations of supervisory authorities