Rambøll Binding Corporate Rules (Compiled version)

For the protection of personal data transfers

Table of Contents

1. WHAT ARE BINDING CORPORATE RULES (BCR)?

These Binding Corporate Rules (hereafter, "BCR") are internal rules adopted by Ramboll Group A/S ("Ramboll") and its participating corporate entities ("Ramboll Entities") that work as the transfer basis for transfer of personal data between covered entities in Ramboll.

A full list of the Ramboll Entities covered by the BCR (incl. countries) can be made available upon request.

Ramboll's BCR present "adequate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals" within the meaning of applicable data protection law, especially the data protection laws of the Member States of the European Economic Area ("EEA").

The BCR is a controller-to-controller BCR, which means that is serves as a transfer basis in situations where a Ramboll entity covered by the BCR acts as a controller and transfers personal data to another Ramboll entity acting as a controller too.

The BCR do not cover situations where a Ramboll entity acting as data controller transfers personal data to another Ramboll entity acting as processor.

You can find the final decision from the European Data Protection Board regarding Ramboll's BCR here: https://www.edpb.europa.eu/system/files/2023-01/edpb_opinion_202232_bcr-c_ramboll_en.pdf

2. RAMBOLL'S TRANSFERS OF PERSONAL DATA

The BCR apply to Ramboll Entities which are processing personal data relating to data subjects:

a) in the EEA or in a country with an adequate level of data protection as acknowledged by a decision of the European Commission; and
b) outside the EEA

The BCR will cover all personal data transferred directly or indirectly out of the EEA to any of the Ramboll Entities. This includes data concerning employees, customers, subcontractors and other third parties processed internally by the Ramboll Entities as part of their regular business activities.

The personal data transferred to other Ramboll Entities will mainly comprise general employee data. The transfers are related to the use of global IT-systems, shared services and for reporting and analysis purposes. HR information is transferred between Ramboll entities for employee mobility and relocation purposes. The transfers also include special categories of personal data, namely health information about employees regarding work related incidents.

3. OVERVIEW OF DATA PROCESSING ACTIVITIES COVERED BY THE RAMBOLL BCR

Processing activities	Purpose of processing	Categories of data subjects	Categories of personal data
HR function	Recruitment, hiring, personnel	Employees, applicants,	Contact information, CVs, applications,

	administration, performance management, employee development, whistleblower arrangements and exit of employees.	consultants, visitors, former employees	employment details, bank information, expenses, usernames and passwords, social security number, performance details, health information,[1], union membership
Customer management	Management of customer relationships, including financial management	Customers	Contact information, customer relationship details
Supplier management	Management of relationships with suppliers and other business contacts, including financial management	Suppliers, other business contacts	Contact information, relationship details
IT services	Provision of IT services to group entities, such as infrastructure services, access management, support and maintenance of IT systems, business intelligence and project management	Employees, applicants, consultants, visitors, former employees, customers, suppliers, other business contacts	Employees, applicants, consultants, visitors and former employees: Contact information, CVs, applications, employment details, bank information, expenses, usernames and passwords (encrypted), social security number, performance details, health information, union membership. Customers: Contact information, customer relationship details Suppliers and other business contacts: Contact information, relationship details

The categories of recipients of the Personal Data are the Ramboll Entities covered by this BCR.

[1] Special categories of personal data are only processed under the BCR, if this is in accordance with applicable Member State law and subject to a Transfer Impact Assessment

4. BINDING EFFECT UPON RAMBOLL ENTITIES

Ramboll's Group Executive Board has decided that the BCR shall be implemented throughout the Ramboll Group. The decision is supported by the Ramboll's Board of Directors. Consequently, the applicable Ramboll Entity has undertaken to adhere to the BCR by having duly signed a legally binding undertaking under which the Ramboll Entity is obliged to adhere to and implement the rules and procedures set out in the BCR.

Accordingly, all the Ramboll Entities and their employees are bound to comply with the BCR including all appendices hereto in respect of any transfer of personal data between Ramboll Entities covered by the BCR. However, non-EU Ramboll entities covered will only adhere to the BCR and fulfil the obligations with respect to personal data transferred directly or indirectly out of the EU or EEA under the BCR.

5. DATA PROTECTION PRINCIPLES

The following principles, which derive specifically from the GDPR and the Madrid Resolution of November 5, 2009, apply and will be enforced with respect to the processing of personal data by participating companies within the scope of the BCR:

5.1 Legitimacy and legality of data processing

The processing of personal data shall be done lawfully in compliance with the relevant statutory provisions under EEA legislation and with due regard for the principles laid down in the BCR.

The processing of personal data by a Ramboll Entity is only permissible if at least one of the following prerequisites is fulfilled:

a) Data subject has consented
b) Processing necessary for performance of a contract
c) Processing necessary to safeguard the legitimate interests of the controller and the legitimate interests is not overridden by the interest of the data subject
d) Processing necessary for compliance with the law of a Member State to which the controller is subject
e) Processing is required, exceptionally, to protect the vital interest, such as the life, health or safety, of the data subject

5.2 Purpose limitation

Ramboll Entities process personal data exclusively for specified, explicit and legitimate purposes and under no circumstances in a way that is incompatible with the legitimate purposes for which the personal data was collected. Ramboll Entities are obligated to adhere to these original purposes when storing and further processing or using personal data transferred to them by another Ramboll Entity.

The purpose of data processing may only be changed with the consent of the data subject or to the extent permitted by the applicable Member State law. This also applies in relation to transfers from a Member State to a Ramboll Entity in a non-Member State.

5.3 Transparency

Each Ramboll Entity commits to make the BCR readily available to every data subject and this shortened, compiled version of BCR are available on Ramboll's website. The full version of the BCR Policy incl. appendices is available upon request.

All Ramboll Entities shall process personal data in a transparent manner. All Ramboll Entities will adhere to the substantive principles for processing personal data set out in this Section 5 and will ensure that data subjects are provided with the information set out in Section 6 of this compiled version of Ramboll's BCR Policy by the relevant Ramboll Entity (in consultation with the transferring company, if applicable). Further, all Ramboll Entities respect and act in accordance with the third-party beneficiary rights set out Section 8.

5.4 Accuracy, data minimisation and data retention

Personal data processed by Ramboll Entities are correct and kept up to date. Appropriate measures are implemented to ensure that inaccurate and incomplete personal data are corrected, restricted or erased.

Ramboll's processing of personal data is guided by the principle of data minimisation to collect, process, and use only such personal data as is required for the relevant purpose of the processing. In particular, the Ramboll Entities will make use of the possibility to anonymise or pseudonymise personal data, provided that the cost and effort involved corresponds with the desired purpose. Statistical evaluations or studies based on anonymized personal data are not relevant for data protection purposes, if such personal data cannot be used to identify the data subject and provided that local law does not stipulate a higher level of protection for anonymized personal data than the BCR.

Personal data, which is no longer required for the purposes for which it was originally collected and stored, is erased. If statutory retention periods apply, the personal data shall be restricted rather than erased.

5.5 Onward transfer of data

The transfer of personal data from a Ramboll Entity to a non-Ramboll Entity (i.e. a company - including, but not limited to, an internal contractor - that is not bound by the BCR) outside the EEA or a Ramboll entity not covered by the BCR is only permissible under the following conditions:

a) the country is deemed to be adequate under Article 45 of the GDPR; or
b) the receiving entity demonstrates that it has an adequate level of protection for personal data within the meaning of Article 46 of the GDPR, e.g. by concluding an EU standard contract (Standard Contractual Clauses 2021/914) or by concluding other appropriate contractual agreements between the transferring and the receiving entity in accordance with Article 46 of the GDPR, or
c) the transfer is permissible under the exceptions defined in Article 49 of the GDPR

Transfers of personal data from a Ramboll Entity to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Furthermore, if the receiving entity is a processor, the conditions set out in articles 24, 25, 28, 29 and 32 of the GDPR must additionally be satisfied.

5.6 Special Categories of Personal Data

The Ramboll Entities may, if required for the purpose of the relevant processing activity, process and transfer Special Categories of Personal Data, namely health information about employees regarding work related incidents. Particular precaution must be taken by each Ramboll Entity if Special Categories of Personal Data are processed.

Should the processing of Special Categories of Personal Data be required, the explicit consent of the data subject must be obtained, unless such processing is expressly permitted by the laws of a Member

State (e.g. for the purpose of registering/protecting minorities), and additional requirements set out in the GDPR are complied with for the processing of Special Categories of personal data, including adequate security measures applicable for the processing of such personal data. Ramboll Entities will not process on the basis of explicit consent under this Section 5.6, where Union or Member State law has made exception to such processing pursuant to article 9 (2) (a) of the GDPR.

5.7 Direct Marketing

The Ramboll Entities will ensure to comply with applicable EEA Member State law and practices in relation to direct marketing and not approach data subjects with direct marketing enquiries without consent from the data subject, unless the data subject has previously bought products or services similar to the subject matter of the marketing enquiry and has not declined receiving such communications.

The Ramboll Entities will inform the data subjects on their right to object to the processing of the data subjects' personal data for advertising purposes or for purposes of market research and/or opinion polling purposes.

The Ramboll Entities will inform the data subject of its right to object free of charge to the processing of the data subject's personal data. In such cases, the Ramboll Entities will refrain from contacting the data subjects who have opted out of receiving marketing information.

5.8 Automated individual decisions

If personal data is processed for the purpose of making automated individual decisions, the legitimate interests of the data subject must be ensured through appropriate measures. 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.

An exception applies only if the decision:

a) is taken in the course of entering into or performance of a contract and is necessary for the one of these, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard the data subject's legitimate interests, such as giving the data subject the opportunity to put the data subject's point of view forward; or
b) is authorized by applicable Member State law which also lays down measures to safeguard the data subject's legitimate interests; or
c) is based on the data subject's explicit consent.

Where the decision is taken in relation to entering into/performing a contract or where the decision is based on the data subject's explicit consent, the Ramboll Entity shall implement the right to obtain human intervention with the Ramboll Entity, to express his or her point of view and to contest the decision.

5.9 Data security

The Ramboll Group has established and documented an IT security organization and has integrated data security into the processes of this organization. The Ramboll Entities will take appropriate technical and organizational measures to ensure data security. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected (privacy by design). Special categories of personal data shall be subject to specific security and protection measures. Such

measures shall further ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed (privacy by default).

Specific measures are used to ensure adequate protection of personal data, including admission controls, system access controls, data access controls, transmission controls, input controls, job controls, availability controls and segregation controls.

Ramboll has implemented a data protection breach procedure setting out how all personal data breaches must without undue delay be reported to Ramboll's Global Data Protection Manager and procedures for how the Global Data Protection Manager must handle personal data breaches, including notification to the relevant data protection authorities and the affected data subjects when necessary.

5.10 Confidentialit

Only Ramboll employees, who are authorized by Ramboll and have been specifically instructed in compliance with data protection requirements may collect, process or use personal data. Access authorization of the individual employee will be restricted according to the nature and scope of the employee's particular field of activity. The employee is prohibited from using personal data for private purposes, from transferring or from otherwise making personal data available to unauthorized persons. Unauthorized persons in this context include, for example, other employees, to the extent that they do not require the personal data to complete their specialist tasks. The confidentiality obligation continues beyond the end of the employment of the employee in question.

5.11 Use of data processors

When a Ramboll Entity as a controller instructs another Ramboll Entity or a third-party legal entity not bound by the BCR (the Processor) to process personal data, the following requirements will be observed:

a) the Processor is carefully assessed and selected by the Controller based on the Processor's ability to ensure the implementation and maintenance of necessary technical and organizational security measures required for complying with the BCR in relation to data processing;
b) the Controller will ensure and regularly verify that the Processor remains fully compliant with the agreed technical and organizational security requirements;
c) the performance of processing by a processor must be regulated in a written agreement in which the rights and obligations of the Processor in accordance with the requirements in Article 28 of the GDPR and on a Ramboll template or an equivalent agreement.

5.12 Records of processing activities

Each Ramboll Entity has established and maintains a record of all categories of processing activities carried out by the Ramboll Entity in accordance with GDPR art. 30. The record is maintained in writing, including in electronic form, and will be made available to an EEA data protection authority on request. The data processing activities covered by the BCR are listed in Section 3.

5.13 Data Protection Impact Assessments

Each Ramboll Entity will assess the risk of its processing activities. When a processing activity is likely to result in a high risk to the rights and freedoms of natural persons, the Ramboll Entity will carry out a data protection impact assessment in accordance with article 35 of the GDPR. The Ramboll entity endeavours to mitigate found high risks. If it is not possible to mitigate the risk, the Global Data Protection Manager will consult the competent EEA data protection authority, prior to processing personal data for the relevant processing activity.

6. DATA SUBJECT'S RIGHTS

6.1 Information obligations

A Ramboll Entity obtaining personal data from the data subject will inform the data subject about the processing in a privacy policy in accordance with the provisions in GDPR art. 13. The information is given at the time when the personal data is obtained.

A Ramboll Entity obtaining personal data from other sources than the data subject will inform the data subject about the processing in a privacy policy in accordance with the provisions in GDPR art. 14. The information is provided within a reasonable period after obtaining the personal data, but no later than one (1) month. If the personal data is used for communication with the data subject, the information is provided at the latest when the Ramboll Entity is first communicating to the data subject. If a disclosure to a third party is envisaged, the information is at the latest provided when the person data is first disclosed to such third party.

If the data subject already has information about how Ramboll processes personal data, it is not necessary to provide the information to the data subject regardless of whether personal data is collected from the data subject or from others.

If a Ramboll Entity at a later stage intends to process personal data obtained from the data subject or elsewhere for a new purpose than stated in the privacy policy, the Ramboll Entity in question will notify the data subject prior to that further processing on the purpose of such processing and provide the data subject with any other relevant information pursuant GDPR art. 13 or 14.

When provided for by applicable law of an EU Member State, the data subject will not have a right to information:

a) If the provision of such information proves impossible or would involve a disproportionate effort (especially processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to comply with and implementing alternative measures as regulated by EU or Member State law)
b) if obtaining or disclosure of the personal data is expressly laid down by EU or Member State law to which the relevant Ramboll Entity is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
c) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or Member State law

6.2 Rights of the data subject

Each Ramboll Entity will ensure that all data subjects will be able to obtain:

a) confirmation as to whether or not personal data relating to the data subject is being processed and the listed information in GDPR article 15, see further in Section 7;
b) restriction of a Ramboll Entity's processing of the data subject's personal data in certain situations set out under GDPR art. 18;
c) the right to any time object, on grounds relating to the data subject's particular situation, where the processing of personal data is based on a balancing of interests; and
d) the right not to be subject to a decision solely based on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her.

The law of a Member State may restrict the data subject's rights set out above, including the right to access if this right is exercised repeatedly within a short period of time, unless the data subject can show a legitimate reason for the repeated assertion of claims for information. Further, Ramboll may

restrict the data subject's right to obtain a copy of the personal data undergoing processing under Section 6.2(b) if the right adversely affects the rights and freedoms of others.

Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Ramboll Entity receiving a data subject access request may charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, for providing the information set out under Section 7.

Further, each Ramboll Entity will ensure that all data subjects may at any time object to Ramboll's processing of data relating to the data subject. Where the objection is justified, each Ramboll Entity will ensure that the personal data is erased and no longer will be processed.

The data subject can assert the above rights by contacting the Global Data Protection Manager.

7. SUBJECT ACCESS REQUESTS

Data subjects whose personal data is collected and/or used in the EEA and/or transferred between Ramboll Entities, as defined in this BCR, will also benefit from the right of Subject Access.

A data subject making a subject access request (hereafter "Request") to a Ramboll Entity under this BCR is entitled to be informed about:

- whether the Ramboll Entity holds and is processing personal data about that data subject.
- the purposes of the processing,
- the categories of personal data concerned,
- the recipients or categories of recipients to whom the personal data are disclosed,
- the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period,
- the existence of the right to request from the Ramboll Entity rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing, the right to lodge a complaint with a supervisory authority,
- where the personal data are not collected from the data subject, any available information as to their source, and
- whether automated decision making, including profiling, will be applied to the personal data, including information on the logic involved in such decision making and the significance and envisaged consequences of such processing.

The information must be communicated in an intelligible form

Without excluding other means of communication, Requests may be in writing and can for an example be submitted via e-mail. The Request must be made by the data subject her or himself and sent to the Global Data Protection Manager. Contact information for the Global Data Protection Manager is listed on Ramboll's website, www.ramboll.com.

Under normal circumstances no fee will be applied by the Ramboll Entities for the processing of the Request.

A Ramboll Entity must respond to a Request within one (1) month of receipt of the Request or within this deadline inform the data subject making the Request when a response will be provided. However, in exceptional cases a response can be provided within three (3) months of receipt of the Request.

The Ramboll Entity may ask for information which the Ramboll Entity may reasonably require in order to confirm the identity of the data subject making the Request and to locate the information which that data subject seeks.

8. THIRD PARTY BENEFICIARY RIGHTS

Data subjects whose personal data is (i) transferred from the EEA to a country outside the EEA by a Ramboll Entity and (ii) is subject to the BCR shall be able to enforce the following third party beneficiary rights against such Ramboll Entity:

a) to seek enforcement of compliance with the BCR, including but not limited to seeking enforcement of the following rights and principles:
   i. the substantive principles for the processing of personal data set out in Section 5;
   ii. the information rights set out in Section 6.1;
   iii. the rights of the data subject set out in Section 6.2;
   iv. local statutory regulations in accordance with Section 10.4;
   v. the right to make a complaint through the procedure set out in Section 11;
   vi. any support of or cooperation needed with data protection authorities pursuant to Section 10.2;
b) to lodge a complaint with an EEA data protection authority, in particular in the Member State of the data subject's;
   i. habitual residence;
   ii. place of work; or
   iii. where the alleged infringement of the BCR occurred; and/or
c) to take action against a Ramboll Entity in order to enforce compliance with the BCR in the courts of the jurisdiction in which:
   i. the Ramboll Entity responsible for the alleged breach is established; or
   ii. the Ramboll Entity responsible for exporting the personal data is established; or
   iii. the data subject has his or her habitual residence; or
   iv. the Ramboll Headquarter is established;
d) to make complaints to a Ramboll Entity within the EEA and, where appropriate, receive compensation from a Ramboll Entity for material or non-material damage suffered as a result of a breach of the BCR in accordance with the determination of a court or other competent authority. Such complaints may be made in accordance with Section 11;
e) to obtain redress and where appropriate compensation from the exporting Ramboll Entity or the Ramboll Headquarter in case of any damages resulting from a breach of the BCR by a Ramboll Entity; and
f) to obtain a copy of the BCR with its Appendices and the Undertaking on request or by obtaining a copy of the BCR on Ramboll's website.

In the event of a claim being made in which a data subject has suffered any material or non-material damage, Ramboll has agreed that the burden of proof to show that (i) a Ramboll Entity outside the EEA is not responsible for the breach, or (ii) that no such breach took place, will rest with the Ramboll Entity responsible for exporting the personal data to a Ramboll Entity outside the EEA.

In addition, claims may be brought against the Ramboll Headquater, i.e. Ramboll Group A/S, that has undertaken to accept responsibility for and agreed to take the necessary action to remedy the acts of other Ramboll Entities outside of the EEA and to pay compensation for any material or non-material damages resulting from the violation of the BCR by Ramboll Entities. In this case the courts or other competent authorities in the EU will have jurisdiction and the data subject will have the rights and

remedies against the Ramboll Headquater as if the violation had been caused in the Member State in which the Ramboll Headquater is based instead of the BCR member outside the EU.

In the event that a non-EEA Ramboll entity is no longer a party to the Ramboll BCR or otherwise ceases to exist, the third-party beneficiary rights provided to data subjects under Section 8 will survive to ensure that the data subject's rights are not affected by such withdrawal from the BCR.

9. COMPLIANCE AND SUPERVISION OF COMPLIANCE

Ramboll has appointed a Global Data Protection Manager who is responsible for overseeing land ensuring compliance with the BCR. The Global Data Protection Manager advises the Group Executive Board, deals with the data protection authorities' investigations, conducts annual reports on compliance, and ensures compliance at a global level. The Global Data Protection Manager is enjoying the support of management of Ramboll for fulfilling these tasks.

Where required under local law, Ramboll will further designate a Data Protection Officer (DPO) in line with article 37 of the GDPR.

10. MISCELLANEOUS

10.1 Audit

The Ramboll Group's audit effort is multi-layered, embedded in existing processes and covers the entire BCR framework and the requirements and activities thereunder.

The Global Data Protection Manager is responsible for the internal audit activities and ensures that the audit activities address all aspects of the BCR, including corrective and preventive actions. The Global Data Protection Manager is responsible for bringing the result of an audit to the attention of the Group Compliance Director, CFO and Ramboll's legal department, Ramboll's Audit & Finance Committee and the board of directors of Ramboll, who are all committed to ensuring that any corrective actions remedying any non-compliance will take place as soon as is reasonably possible.

The BCR is audited annually and at the request of the Global Data Protection Manager. The scope of the audit is decided based on a risk and materiality assessment. Other audit activities are carried out according to predefined schedules but no later than within 3 years of the BCR being adopted. The Ramboll Entities will provide copies of the results of any audit of the BCR to EEA data protection authorities upon request.

10.2 Cooperation with the EEA data protection authorities

The Ramboll Entities will cooperate and support any personal data protection authorities in the event of inquiries and complaints from data subjects.
Where required, the Ramboll Entities will make the necessary personnel available for dialogue with an EEA data protection authority in relation to the BCR.

Further, the Ramboll Entities will comply:

- with the decisions made by the EEA data protection authorities on any issues that may affect the BCR or any issues related to the interpretation and application of the BCR, and
- with the views of the European Data Protection Board as outlined in its published guidance on binding corporate rules.

10.3 Training

The Ramboll Entities will provide appropriate training to employees who have permanent or regular access to personal data or who are involved in the collection of personal data or in the development of tools used to process personal data.

10.4 Relationship between BCR and local statutory regulations

Prior to a transfer of personal data taking place, the data exporting Ramboll Entity with help of the data importing Ramboll Entity, will, taking into account the circumstances of the transfer, evaluate, if local legislation, regulations, statutes, court orders or mandatory standards (hereinafter "Local Legislation") will prevent the Ramboll Group from fulfilling its obligations under the BCR and determine any required supplementary measures to be taken.

Before any updated Local Legislation comes into force and where the transfer already takes place, the data exporting Ramboll Entity with help of the data importing entity will evaluate, if the updated Local Legislation will prevent the Ramboll Group from fulfilling its obligations under the BCR and determine any required supplementary measures to be taken.

Ramboll's Global Data Protection Manager, will inform and advise the Ramboll Group on the documented investigation and any proposed supplementary measures.

Where Local Legislation requires a higher level of protection than is contemplated under this BCR, such Local Legislation will take precedence over this BCR, and the processing will be made in accordance with the Local Legislation.

Where the evaluation of Local Legislation requires supplementary measures, the Ramboll Group will implement those. However, if no supplementary measures can be put in place the Ramboll Group must suspend the transfer; if the Ramboll Group decides to continue the transfer, the relevant EEA data protection authority(ies) will be notified.

The outcome of the evaluation and proposed supplementary measures will be properly documented and kept at the disposal of the EEA data protection authority(ies).

Where a Ramboll Group member has reasons to believe that any legal requirement the Ramboll Group is or may become subject to in a third country prevents or may prevent the Ramboll Group from fulfilling its obligations under the BCR or has or may have substantial effect on the guarantees provided by the Data Protection Legislation, including any legally binding request for disclosure of Personal Data by a law enforcement authority or state security body, the Ramboll Entity will promptly inform the Global Data Protection Manager who will report such problem to the competent EEA Supervisory Authority (except where prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In specific cases where the abovementioned notification is prohibited, the relevant Ramboll Group member will use best efforts for such prohibition to be waived. If, despite its efforts, the requested Ramboll Group member is not in a position to notify the competent EEA data protection authority(ies), it will annually provide general information on the requests it received to the competent EEA data protection authority(ies).

10.4.1 Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance

treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to Chapter V of GDPR.

11. RAMBOLL BCR COMPLAINT MECHANISM

According to the current requirements by the EEA data protection authorities in the Member States, the Ramboll Group is obliged to implement a complaint handling procedure as part of the BCR.

Data subjects can report complaints by contactingthe Global Data Protection Manager. Complaints can be made to privacy@ramboll.com. Further, contact information of the Global Data Protection Manager and further information as to how to make complaints is available on Ramboll's website, www.ramboll.com.. Without excluding other means of communication, complaints may be in writing and can for example be submitted via e-mail.

The Global Data Protection Manager is responsible for and will handle the complaint in a diligent and efficient manner and take all relevant steps to handle the complaint according to the BCR and the law of the Member State in which the Ramboll Entity to which the complaint was submitted is established. The complaint handling procedure will include involving relevant employees within the Ramboll Entities and, if necessary, by external advice.

12. UPDATE OF THE RULES

Ramboll's Global Data Protection Manager will keep track of and record any updates to the BCR and provide the necessary information to the data subjects or EEA data protection authorities upon request. Ramboll will without undue delay communicate any material changes to the BCR to the Danish Data Protection Agency (in Danish: "Datatilsynet") and any other relevant EEA data protection authorities.

Ramboll will also provide a brief explanation of the reasons for any notified changes to the BCR. Ramboll will once a year provide the Danish Data Protection Agency with an overview of changes made, which are not considered to be substantial.

Ramboll will without undue delay communicate any changes to the BCR to the Ramboll Entities bound by the BCR and to relevant data subjects who benefit from the BCR. The BCR contains a change log, which sets out the date the BCR is revised and the details of any revisions made.

Ramboll's Global Data Protection Manager will maintain an up to date list of the Ramboll Entities bound by the BCR and ensure that all new Ramboll Entities are bound by the BCR and can deliver compliance with the BCR before a transfer of personal data to them takes place.