Wallenius Wilhelmsen

# Binding Corporate Rules

## Global Privacy Policy

**Legal notice:** Our BCR is sent in for approval by the Norwegian data protection authority (Datatilsynet) and is currently under review. This version of the BCR shall be considered a draft version (subject to changes) until it is approved by the authorities. The BCR were published on the 25th of May 2018 to fulfil our legal obligation (General Data Protection Regulation) on informing individuals subject to our personal data processing activities and is the Wallenius Wilhelmsen group's internal global privacy policy. Any individuals' rights and our obligations due to the General Data Protection Regulation is valid regardless of the BCR application process.

Version: 2

# Table of contents

**APPENDIX:**

WW Group BCR - Intra-Group Agreement

# 1 Introduction

## 1.1 About this document

The Wallenius Wilhelmsen Group (WW Group) employs approximately 7,500 employees in 29 countries worldwide. The WW Group consists of the ultimate parent company Wallenius Wilhelmsen ASA and its subsidiaries. The subsidiaries can be divided into four cores:

- Wallenius Wilhelmsen Ocean, which owns and operates a fleet of approximately 130 Ro-Ro vessels;
- Wallenius Wilhelmsen Solutions, which provides landbased logistics solutions;
- EUKOR Car Carriers Inc., a major Korean Ro-Ro carrier; and
- American Roll-on Roll-off Carriers, a stand-alone North American Ro-Ro carrier.

The WW Group aim to provide the same level of data security and privacy rights globally. The Binding Corporate Rules / Global Privacy Policy (BCR) shall be made available to customers, employees and others who may have a relation to the WW Group. Therefore, the aim is to make the BCR as easily understandable as possible to enable individuals to exercise their data privacy rights. For a quick overview of rights, please confer sections 7, 8, 9. Kindly note that the rules and rights are written in so-called 'legal language' to comply with the European Union General Data Protection Regulation (GDPR) hence any reader must use the definition list in section 3.

## 1.2 General information about the Binding Corporate Rules

For implementing the new set of standards imposed by the GDPR, the WW Group has set up new internal standards for personal data protection. The BCR will make these standards binding by contractual means and make the mother company, Wallenius Wilhelmsen ASA, liable for any breaches of the rules by any member of the group outside of the EU/EEA. The binding character of the BCR are ensured by intra-group agreements with relevant group-companies outside EU/EEA, making the policy and relevant procedures scope global. At employee-level, the rules are made binding by an internal global policy with sanctions up to and including immediate dismissal.

The existence of the BCR enables individuals (data subjects) to exercise their rights regardless of where their personal data is being processed. In a big-scale global company this is needed for having personal data privacy in practice, since it creates a chain of accountability no matter if your data is obtained or contained in Norway, Germany or in for example Thailand.

For the EU/EEA, the BCR will be used as an internal policy, without keeping the EU/EEA companies bound by an intra-group agreement. This is possible since the companies abide the same set of European laws.

# 2 List of companies bound

A list of current WW Group companies bound by the Binding Corporate Rules can be found by visiting:

www.walleniuswilhelmsen.com/privacypolicy

The list of companies is updated regularly by the lead supervisory authority (DPA) and the Norwegian Data Authority (Norwegian: Datatilsynet), will be noticed directly if any major changes affecting data subjects or general data privacy occur. Regardless, once a year, a current list of companies will be submitted to Datatilsynet to enable their supervision. The responsible person for keeping the list and the DPA updated is the WW Group's appointed DPO.

## 2.1 Data Transfers to bodies not bound by the Binding Corporate Rules

Any data transfers to any WW Group third country-companies not legally bound by the BCR is strictly prohibited.

# 3 Definitions

In these Binding Corporate Rules:

"**Binding Corporate Rules**" or "**BCR**" means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

"**Biometric Data**'" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

"**Bound Company**" means any company bound by the BCR;

"**Consent**" means any freely given, specific, informed and unambiguous indication of a data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

”**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;

“**Cross-border Processing**” means either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

”**Data Concerning Health**” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

”**Data Protection Officer**” means the same as in the GDPR;

“**DPO**” means Data Protection Officer;

”**Enterprise**” means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

”**EU**” means the European Union;

”**EU/EEA**” means the EU, the European Economic Area and Switzerland;

”**Filing System**” means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

”**Genetic Data**” means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

”**Group of Undertakings**” means a controlling undertaking and its controlled undertakings;

”**HQ**” means the public limited liability company Wallenius Wilhelmsen ASA with company registration number 995 216 604 and registered offices at Strandveien 20, Lysaker, Norway;

”**Information Society Service**” means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1);

”**International Organisation**” means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

”**Main Establishment**” means: (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

”**Personal Data**” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

”**Personal Data Breach**” 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;

”**Processing**” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

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

”**Profiling**” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

“**Pseudonymisation**” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

”**Recipient**” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

”**Relevant and Reasoned Objection**” means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

”**Restriction of Processing**” means the marking of stored personal data with the aim of limiting their processing in the future;

”**Representative**” means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

”**Third Party**” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

”**Supervisory Authority**” means an independent public authority which is established by a Member State pursuant to Article 51;

”**Supervisory Authority Concerned**” means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority; and

”**Wallenius Wilhelmsen Group**” means the global group of entities which is under the control of HQ.

# 4 General Compliance

Any company within the WW Group shall comply with the BCR and any procedures related hereto. In addition to the BCR, a WW Group company may have to comply with additional national laws and regulations for data processing, competition law or other. If such national regulations prevent compliance of the BCR, this needs to be reported to the WW Group appointed DPO, who shall decide how to proceed and contact the lead supervisory authority (if necessary). Any such decisions shall be documented and made available to the relevant supervisory authorities if requested.

If any WW Group company becomes involved in any data privacy procedure involving supervisory authorities, the WW Group appointed DPO shall be informed and involved.

All employees in the WW Group shall have sufficient knowledge of and comply with the BCR. Depending on which tasks they carry out, different levels of knowledge are required for compliance.

If an employee notices a procedure that may be in breach with the BCR, the employee shall notify his or her manager. The manager shall contact the WW Group appointed DPO. Any employee may also notify the WW Group appointed DPO directly of any breaches or possible breaches. Any such notification or whistle-blowing shall never be punished in any way.

WW Group enforce the compliance of the BCR on its' employees by taking appropriate measures against individuals who breaches the Policy. An employee will always be treated with respect and care if investigated for breaches of data privacy regulations. The employee can always provide his or her version of the happening(s) and strict care will be taken to ensure legal certainty in any such investigation. If an employee is found to have breached his or her obligations, this may result in sanctions up to immediate termination. This provision does not restrict any other legal measures.

**Relevant internal document:**

Global Employee Privacy Policy

## 4.1 National laws preventing compliance and disclosures to authorities

If a WW Group company or an employee knows or believes that national legislation will prevent it from fulfilling its obligations or guarantees of data privacy in this BCR or the GDPR, the said company need to promptly inform the WW Legal & Compliance department and WW Group appointed DPO. The only exception on this rule is if the notification would be illegal due to confidentiality by for example a criminal investigation.

If a national legislation (also in the EU/EEA) prevents a WW Group company as above and this may create privacy infringements for data subjects, the WW Group appointed DPO will report this to the national competent supervisory authority (Datatilsynet) and provide information of the issue – including but not limited to: if any personal data has been disclosed, who it has been disclosed to and information about the national legislation who infringes the compliance. This could for example be if a WW Group company need to provide a third country-authority with personal data during a criminal, competition or any other investigation. Any such disclosure need to be documented.

- If a WW Group company submits personal data to authorities, the company should always strive to keep the personal data minimalistic and use its best efforts to protect individuals from unwanted disclosures.

Every year a bound company need to provide the WW Group appointed DPO with a report on personal data disclosures to authorities. This need to be at least:

- Number of disclosures.
- How many persons affected.
- What type of personal data.
- Who it was sent to (if not illegal due to confidentiality).

If a bound company believes that their transfers infringes a data subjects' rights in any way, the internal Report form for authority disclosures need to be filled and made available to the WW Legal & Compliance department and/or the WW Group appointed DPO.

Any transfer of personal data to any public authority can never be massive, disproportionate or indiscriminate in a manner that goes beyond what is necessary in a democratic society.

# 5 Duty to co-operate with DPA

Any bound company have a strict duty to co-operate with any competent European supervisory authorities regarding the provisions and rights in the BCR. This may include responding to requests of in-sight, follow up on advices or follow their decisions in relation to applicable data privacy laws. The WW Legal & Compliance and the WW Group appointed DPO shall be informed of any such co-operation if not prohibited by law. This will enable the WW Group to quickly undo or restrict any harm to data subjects.

The WW Group will inform the relevant supervisory authority of any major changes to the BCR or the list of bound companies in an urgent matter. Minor changes shall be notified at least once a year.

# 6 General Information on WW Group processing

## 6.1 Processing activities

The WW Group processes personal data of current and former employees, contractors, persons applying for jobs, customers, suppliers, newsletter subscribers, website users (see Cookie Policy), physical guests and shareholders.

## 6.2 Purpose of processing

WW Group may process personal data about individuals for the following purposes:

*Administration, human resources and management of employees/personnel;*

These purposes includes processing that is necessary for the performance of an employment contract or a prospective employment contract, including but not limited to processing related to recruitment and deployment, performance and development, management and administration of payments, compensation, benefits and reward, tax issues, career planning, evaluations, training, travel and expenses, outplacement, communication with personnel, employee relations, change management and continuous improvement.

*Health, safety and security*;

This purpose includes processing that is necessary to protect health, provide safety and security related to employees/personnel and their next of kin or the public.

*Planning and control measures*;

This purpose includes processing related to activities such as scheduling timetables, recording time, conducting surveys, controls, internal audits and investigations.

*Business operation and protection of business interests and security*;

This purpose includes processing in relation to business operations and protection of business interests and security; e.g. information security, logging, conduction of controls, surveys, analysis, reports and managing of daily operations and transactions/possible transactions involving the WW Group.

*Compliance with legal obligations and protection of legal position*;

This purpose includes processing of personal data that is necessary in order to ensure compliance with legal obligations and/or to protect a legal position of the WW Group.

*Marketing or business-oriented processing*;

This purpose includes processing of personal data that is necessary for direct or indirect marketing to customers, old customers or possible customers. This also includes measures for building or managing external relationships.

*Contractual purposes*;

This purpose includes processing of personal data to fulfil a current, future or prospective contractual relation with customer employee, supplier or likely.

*Other purposes;*

This purpose is not to be seen as a general purpose, but if the WW Group have legitimate, necessary and purposeful needs to process data that does not in a disproportional way infringes someone's right to privacy – this general purpose may be used, with care.

# 7 Personal Rights

Data subjects are always able to enforce their personal rights according to the current legislation. Regarding this matter WW Group intend to particularly inform data subjects of its enforceable rights, either as data subjects according to the GDPR, or as third-party beneficiaries through BCR and the Intra-Group Agreement.

## 7.1 Data protection principles

Any personal data processed need to be lawful, fair and transparent to the data subject.

In this section WW Group provide the relevant legal rules followed by easily understandable explanations to enable data subjects to exercise his/her rights – and to create better understanding for the WW-Groups employees.

A WW Group entity may only process personal data if all of the following data protection principles (this section) and at least one legal basis (section 7.2) are applicable:

### 7.1.1 Data Protection by Design and by Default

All companies bound by the BCR need to continually adopt measures and always when for example conducting M&A, buying IT or HR-services strive to respect the data protection principles in its business decisions. This also creates a duty to continually control systems and procedures regarding the handling of personal data.

An example of data protection by default is to always strive to collect minimal personal data in IT-applications, and the administrator asking itself "is this information needed?". The administrator also need to not grant access to employees if they do not have a qualified need. When handling personal data, WW-Group companies and its employees need to assess whether the information is "good to know" or "need to know".

### 7.1.2 Purpose Limitation

When processing personal data, companies bound by the BCR shall always have a specified, explicit and legitimate purpose and the data shall not be further processed in a manner that is incompatible with those purposes;

Any personal data collected shall only be used for the specific purpose at the time when it was collected. For example: Data collected when employing a person can never be used for marketing, if not agreed specifically. The purpose may not change without explicit, clear consent from the affected data subject. See section 6.2 regarding purposes for processing.

### 7.1.3 Data Minimisation

The personal data needs to be adequate, relevant and limited to what is necessary to achieve the purpose for which they were processed;

The personal data collected shall always strive to be as minimalistic as possible. If there is no purposeful use of the personal data – it shall not be collected. Data already collected that does not fulfil this criterion shall be erased. For example: A picture of a person which was sent in when applying for a job is not necessary to keep when the application procedure is completed.

### 7.1.4 Limited Storage Periods

Connecting to the above principle of Data Minimisation: Personal data shall not be kept for longer than is necessary for the purposes for which the personal data are processed;

Personal data shall have limited storage periods connected to the purpose for which they are kept. This creates a need to have different set of storage times on different data. For example: Personal data of pay checks or other contractual documents can be kept for longer than the previous example of pictures of the employee. A pay check may be needed for accounting-purposes in several years while a picture of a former employee/candidate should be deemed purposeless quite fast.

### 7.1.5 Data Quality/Accuracy

The personal data processed shall always strive to be accurate and up to date;

If the data becomes inaccurate and thus purposeless it should be either rectified or erased.

## 7.2 Legal bases for Processing

To be able to comply to the principles of processing personal data, bound companies need to always have a lawful basis.

There are six different lawful bases (as described in the following), at least one must always apply.

### 7.2.1 Consent by the data subject

The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

If a data subject consents to processing, the consent need to fulfil the legal requirements of: documentation, separate terms, a clear commitment by the data subject, clear and plain language, clear purposes and use of the data, possibility to withdraw the consent, and more. Furthermore, the consent need to be refreshed by the data subject it the terms are changed. This altogether makes consent a complicated legal ground for a logistic company mainly doing business B2B, since it may be hard to get the data subject to comprehend what he/she agrees to. Therefore, any consent-request must be done with strict care, and mainly for marketing purposes.

### 7.2.2 Contractual ground

The 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;

If the bound company have a contract with the data subject and it's necessary to process their personal data for complying with legal obligations, administrative measures or to ensure that the contract can be fulfilled. This also applies in a pre-contractual phase, to be able to later enter into a contract.

### 7.2.3 Legal obligation for the bound company

The processing is necessary for compliance with a legal obligation to which the controller is subject;

If the personal data is needed to comply with a legal obligation, the personal data can and must be processed. However, the processing needs to be necessary, if it's possible to comply with the legal obligation without processing the personal data this should be prohibited.

### 7.2.4 Processing to protect the data subject or others

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

When processing for example records about an employee's food-allergenics to be able to serve correct food, this is a justifiable and necessary cause. However, processing data of allergenics not related to the employment is not. Another example could be to do what is necessary to help an employee during an emergency.

### 7.2.5 Public interest

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;

The bound companies can only rely on this legal basis if they either exercise official authority or carries out tasks in the public interest.

#### 7.2.6 Legitimate interests

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;

The bound companies should avoid using this legal ground if another applies, since it's hard to comply with the principles in section 7.1, however, it can be used if it's deemed purposeful, necessary and does not override the data subjects right to privacy. The interests of the bound company and the data subject must be balanced in a reasonable matter.

## 7.3 Processing of special categories of personal data

The WW Group shall not seek to process below sensitive personal data if not absolutely necessary:

- Racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership(s), genetic data, biometric data (used for ID purposes), health, sex-life, criminal records or sexual orientation.

The list above is not exhaustive, other strictly private personal data may be deemed as sensitive as well and need to be handled as such.

When above categories of data are collected, this need to follow the normal rules for data processing, in addition the below requirements need to be met:

- Explicit consent asked for in an easily accessible form using clear and plain language;
- The information is needed to fulfil legal requirements in employment, social security or social protection law;
- The processing is necessary for protecting the vital interests (for example personal security) of the data subject; and
- The processing is necessary for establishing, exercising or defending legal claims.

Whenever sensitive personal data is being processed, the WW Group entity shall seek to always protect the sensitive personal data with high-end encryption and follow procedures in IT security policies, for example on extra strict access control.

## 7.4 Enforceable rights

The WW Group shall assist data subjects when exercising his or her personal enforceable rights according to the BCR and/or applicable national law.

### 7.4.1 Right to access and information

A data subject has a general right to know what personal data is stored about him or her and other information about the processing. In particular this right includes:

- A confirmation that their personal data is stored; and
- If requested: access to the personal data

The information shall be provided free of charge and by the most convenient and safe way possible. The data need to be provided without undue delay with a maximum limit of one month. However, in exceptional cases, taking account the number and complexity of the requests, three months could be acceptable. In the case that the request cannot be dealt with within one month, the data subject must be provided with the reason(s) for delay.

It is of great importance when granting “right to access” to identify the requesting person as the data subject. If not, and the data is submitted to anyone else, this shall be seen as a “personal data breach” which is a major event and need to be addressed by using the global internal data breach procedure.

### 7.4.2 Right to restriction and objection of processing

In some cases, a data subject may have a right to restrict processing of his or her personal data.

The right to restriction means that the bound company stops the processing of the data subjects personal data, instead of erasing it.
The right to restriction applies if any of below numbers (1-4) is fulfilled:

1. The data subject questions the accuracy of their personal data, and bound company uses its one month to verify it;
2. The data has been unlawfully processed and the data subject wants the data restricted instead of erased.
3. The data is not needed by the bound company, but the data subject tells bound company that he/she needs it in order to exercise or defend legal claims; or
4. The data subject has objected to processing made by bound company on the legal ground of legitimate interest (see section 7.2.6), and bound company assesses whether it is necessary to keep the personal data or not.

- As a standard procedure in the WW Group, data should, if practically possible, be restricted while handling a request of exercising any right in the BCR.
- A request regarding restriction or objection of processing can be made both verbally or written. To ensure that a verbal request is followed up, the employee receiving the request shall contact the bound company's relevant data owner (for example bound company's marketing department) in first hand. The data subject may also contact the DPO.

### 7.4.3 Right to rectification and erasure

If the individual data subject has requested his or her information, or by itself know that the personal data kept by a bound company is inaccurate – he or she should be able to have the inaccurate or incorrect data rectified within one month. In some cases, a bound company is able to deny a request, but the main rule is that inaccurate data should be rectified without undue delay. If the personal data is deemed as not purposeful it may instead be erased. The data subject need to be communicated regardless. See section 7.1.5 regarding the accuracy principle.

The right to erasure of personal data may apply to data subjects if any of below (1-7):

1. The purpose of processing the data has become inaccurate;
2. The processing is based on the data subjects consent, and the data subject choses to withdraw this consent;
3. The processing is based on legitimate interest and the data subject challenges this by asking for erasure. If the legitimate interest can't override the data subjects right to erasure/objection the data should always be deleted. If not: The data subjects right to complain to supervisory authorities or court should be communicated without delay;
4. The processing is made for direct marketing purposes;
5. The processing is unlawful;
6. Legal or contractual obligations for the bound company to erase;
7. The data subject is a child;

- When a data subjects request to delete personal data is granted, the bound company need to control whether the personal data have been made available to others than the bound company and ensure that they also delete the data. This could for example be external data processors.

- Before erasing personal data, the WW Group need to be assured that there is no legal obligation on the entity within the WW Group to keep the data. For example, by competition or tax law. It is also of importance to make sure that the WW Group does not need the information for future or ongoing legal claims.

#### 7.4.4 Right to not be subject to decisions based solely on automated processing, including profiling

This right is partly directed on marketing, which is the most relevant for a logistic company.

An individual has an absolute right to not be subject to marketing if he or she withdraws his or her consent.

Automated decision-making and profiling is only permitted if any of the below (1-4) applies:

1. Necessary for entering into or performance of a contract with the individual;
2. Authorised by law;
3. The individuals explicit consent; or
4. If the data processed is deemed sensitive, the data can only be automatically processed with the data subjects explicit consent.

- If a bound company obtains personal data of a data subject for marketing purposes, the bound company needs to provide a link to the WW privacy page, informing the data subjects of his or her rights and a direct link where he or she can unsubscribe.

## 7.5 Right to complain through the internal complaints mechanism

Anyone whose personal data is being processed or believe that their personal data is being processed by WW Group companies may submit a data privacy complaint if he/she believe that a WW Group or any of its employees are infringing personal rights according to the BCR or applicable laws.

The complaint should be directed to the bound company's Legal function. If there is no such local privacy or Legal function available, the complaint can always be directed to the Legal & Compliance department and/or the WW Group appointed DPO function at global level. The complaint should be written or made by appointment with any of the above functions or departments.

- No WW Group employee shall suffer any prejudice, sanctions or any other negative consequences for having submitted a data privacy complaint or any other complaint regarding personal data privacy.

### 7.5.1 Internal procedure in short

Procedure when a complaint is filed against an entity within WW Group:

- WW Group entity receives a complaint.
- Bound company assess whether the complaint is directed to them locally or if the scope of the complaint is global.
- Regardless, bound company contacts the WW Group DPO function stating that he/she received a complaint, the nature of the complaint (for example local or global) and provides a copy.
- The WW Group appointed DPO decides on how to proceed.
- The local or global privacy function (depending on severity of the complaint) will follow the internal global policies and procedures and answer the data subject within one month.
- A bound company should note that if the complaint is directed towards a specific employee, this person should be notified (following the BCR and internal policies) that the bound company or the DPO function may collect personal information relevant to the complaint and may have an internal investigation resolving the complaint. Any employee subject to investigation must be made aware that he/she at any time may provide his/her views and explanations regarding the complaint.

### 7.5.2 WW Groups duty to answer

Whenever a complaint is concluded by the DPO function, regardless of granted or not, the report of the handling should be sent to:

- Local department or person receiving the complaint.
- The person who complained.

The person who filed the complaint shall always, regardless of the result of the complaint, be informed of his or her right to complain to the supervisory authority (Datatilsynet) and his or her right to judicial remedies (section 7.6).

### 7.5.3 Result of a justified complaint

If a personal data complaint is justified, the WW Group appointed DPO shall follow up and take action by giving the bound company support in all reasonable ways to avoid future breaches and remedy the data subject, if this is required by relevant laws or regulations. The following is needed whenever a complaint is justified:

- Notification to WW Legal & Compliance team to address the non-compliance.
- Notification to the employee(s) involved in the complaint.
- The relevant manager to avoid future mistakes or inform him or her that he or she does not follow the BCR, and possible consequences of such non-compliance (see section 9.4 on sanctions towards employees)
- If the granted breach is of serious nature, the WW Group appointed DPO shalll notify the supervisory authority (Datatilsynet)

### 7.6 Judicial remedies

Any data subject who believes the WW Group, its external contractors or service providers infringes his or her rights according to law (EU/EEA companies) or for non-EU companies, the BCR, may lodge a complaint to the relevant supervisory authority or to the Court of the European Union.

A data subject may file a complaint to the supervisory authority in the EU/EEA member state of his or her habitual residence, place of work or the place of the infringement.

A data subject will obtain redress if the WW Group breaches its' legal rights to privacy.

A data subject may, depending on the breach and legal outcome, receive compensation from the WW Group for breaching its' personal rights the according to EU GDPR (EU/EEA) or the Binding Corporate Rules (third countries). Any case regarding a third country and/or third-party beneficiaries, the GDPR rules shall be used as if the violation occurred in the EU/EAA jurisdiction, without prejudice of the BCR formulations.

## 8 How do I exercise my personal rights?

As a data subject you can exercise the principles and rights in section 7 of the BCR. This may be done by either contacting a competent company employee, or by filing a complaint and provide it to either the local bound company or to the WW Group appointed DPO.

The bound company is in first-hand responsible for answering such requests in a rapid matter and resolve the matter if possible. If the bound company seem unwilling, is not responding or do not follow the provisions in the Binding Corporate Rules, please contact the DPO for assistance. Depending on which right, the severity and complexity of the complaint or request, the handling of your issue could take up to 1 or 3 months. However, the WW Group always aim to provide you with an answer as soon as possible.

When exercising your legal rights, always make sure to provide as much information as possible about the issue, your claims and prove that you are you. If we cannot make sure that

you are requesting your own information, we cannot give you any personal information for security and privacy reasons.

# 9 Data Security and legal obligations

WW Group operates globally and needs instant availability of reliable information, including personal data. It is therefore of utmost importance to protect and secure information resources against potential threats.

Most security breaches are due to negligence from companies' own employees. It is therefore imperative to ensure a common understanding of the importance of a conscientious attitude towards security matters and the adherence to security policies, standards and guidelines. For personal data, the WW Group has created training programs to adhere to this need regarding its employees. All employees that regularly handle personal data shall go through internal training programs provided by WW Group HQ in Oslo. The training programs provided contain various degree of details to fit different types of employees and are made available through global managers in each division.

**Relevant internal documents**:

Information Security Policy

Internal computer-based training programs

## 9.1 Personal data to external service providers

Whenever personal data are sent from the WW Group (controller) to any other companies (data processors) not bound by the global privacy policies or BCR, the personal data must be governed by a personal data processing agreement. These agreements need to set clear rules for how the external entity should handle the data (including onward transfers) and make sure that WW Groups internal privacy rules are respected when it leaves the WW Groups direct control.

The requirement of data processing agreements when handling personal data creates a duty to always assess whether the external company is suitable for handling the specific type of data. Typical criteria's when assessing this is how sensitive the personal data is and the quality of security measures and general compliance by the data processor. In other words, "sufficient guarantees" shall be provided by the external data processor before the personal data leaves WW Groups direct control. Any external data processor should be able to submit audits to enable the WW Group appointed DPO or local Legal department to assess whether they are suitable to continue handle WW Group personal data.

Any signed Data Processing Agreements containing personal data shall be submitted to the local Legal departments DPO function to enable reviews, amendments or even terminations.

**Relevant internal document:**

Data Processing Agreement Template

## 9.2 Data Breach Procedure

The global data breach procedure focuses on personal data breaches and give guidelines for practical handling of such, enabling the WW Group to comply with reporting (within 72 hours) and handling data breaches in a consistent, transparent, fair and lawful matter. In the event of a breach by a WW Group company, third-party service providers or other entity or personnel under WW Group control, the affected WW Group company shall notify the DPO and WW Legal & Compliance as soon as possible. The DPO, the affected WW Group entity and the WW Group HQ in Oslo shall use all remedies available to resolve the breach and avoid damages to data subjects.

**Relevant internal document**:

Data Breach Procedure

## 9.3 Global Employee Data Privacy Policy

If an employee breaches its legal obligations for personal data privacy, the following sanctions (1-5) may apply. Any sanction will follow the relevant national laws, including but not limited to employment laws. Any strict sanction (3-5) will need to be thoroughly investigated and motivated legally before imposed upon an employee.

An employee shall always be treated with respect and care if investigated for breaches. He or she can always provide his or her version of the happening(s). Strict care will be taken to ensure legal certainty in any such investigation.

1. Verbal notification from HR or DPO with notification to manager or higher level,
2. Written notification from HR or DPO with notification to manager or higher level,
3. Less career development opportunities and promotions,
4. Reduction of variable pay schemes (if applicable),
5. Termination of the employment contract.

### 9.4 HQ accepts liability for bound entities

In certain jurisdictions (including the EU/EEA) the law prevents international transfers without adequate safeguards in place. The Intra Group Agreements between WW Group entities provide "adequate safeguards" and thus enable lawful international transfers of personal data by making the BCR contractually binding. This ensures individuals that their data and their legal rights is protected no matter where (which country) in the group their data is processed.

If a third country (non EU/EEA) bound entity violates the BCR, the courts or other competent authorities in the EU/EEA will have jurisdiction and the data subject or authorities may direct his/her/its claims directly to the WW Group, as if the infringement had been committed by WW Group HQ in Oslo. WW Group HQ in Oslo shall be exempt from this liability, in whole or in part, only if it can be proved that the bound entity is not responsible for the event giving rise to the damage.

## 10 Transparency and easy access to Binding Corporate Rules

Every bound company aimed towards customers or other private persons shall provide a link to the privacy page at www.walleniuswilhelmsen.com/privacypolicy on their external web-page and provide it by other means (for example by e-mail or hand-outs) if asked for.

## 11 Audit programme

The global data protection audits are conducted internally by the DPO with support of the WW Legal & Compliance, Oslo or the bound entity affected by the audit. Any bound company and its managers need to provide assistance and allocate resources to enable effective audits whenever requested. If decided by WW Legal & Compliance or the DPO-function, professional external auditor firms may be used.

The WW Group data protection audit programme covers all aspects of the BCR and shall be conducted annually to ensure compliance.

The audits allow WW Group DPO function to gain access to its bound companies' personal data and procedures to ensure compliance with BCR or relevant laws.

The DPO function shall directly communicate the results of the audits to the ultimate parent's board at Wallenius Wilhelmsen ASA.

## 12 Data Protection Officer

The DPO: s primary role is to enable compliance with personal data protection legislation. This includes collecting information from managers and employees handling personal data on a

regular basis as well as monitoring compliance in systems. To ensure enforcement of the privacy standards;

1. The DPO shall not receive any instructions from higher level regarding the exercise of his or her tasks;

2. The DPO shall never be penalised or dismissed for performing his or her tasks;

3. The DPO shall report to the highest level of management, when necessary, the DPO shall produce reports and present them to the board of Wallenius Wilhelmsen ASA, Oslo;

4. The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks.

The DPO may fulfil other tasks and duties as long as they do not result in a conflict of interest.

Data subjects may contact the DPO directly regarding all issues related to the processing of his or her personal data, and the rights according to the GDPR legislation.

www.walleniuswilhelmsen.com/privacypolicy

dataprivacy@walleniuswilhelmsen.com

## 12.1 Tasks of the DPO

1. To inform and advise WW Group entities and their employees regarding processing of personal data.

2. Monitoring compliance with data protection legislation and this policy.

3. Organize or conduct training for employees.

4. Conducting internal audits and monitoring external services compliance.

5. Assist, monitor and follow up on data protection impact assessments when required or when the DPO believes it may be required.

6. Direct contact and co-operation with the supervisory authority (Datatilsynet, Norway).

7. Other means of ensuring compliance, including but not excluded to using external auditors, conducting “data breach simulations”, random controls of procedures.

8. Assisting data subjects when exercising their rights.

This creates a duty for all WW Group entities to co-operate with the DPO by:

- Involving the DPO in a properly, timely manner in all issues which relate to the protection of personal data.
- Providing support and resources enabling the DPO: s tasks as above.
- Allowing changes or even terminations of agreements and services if they inflict or risk to inflict damages to data subjects or compliance with legal obligations and these Binding Corporate Rules.

**APPENDIX:**

1. WW Group BCR - Intra-Group Agreement

# WW Group BCR

## Intra-Group Agreement

This Document is a copy of the signed Intra-Group Agreement

This Agreement is valid from: 25 May 2018

The Agreement is valid between parties (1) and (2):

1. Wallenius Wilhelmsen ASA, Norway, Company number: 995 216 604
2. Insert Group Company, Country, Company number: XXXX

The parties are members of the Wallenius Wilhelmsen Group, a global logistics company with its Headquarters in Lysaker, Norway. The relevant supervisory authority is the Norwegian Datatilsynet.

Party 1 title, name:

_____

Party 1 signature:

_____

Party 2 title, name:

_____

Party 2 signature:

_____

## 1. INTRODUCTION / PURPOSE

Due to the Wallenius Wilhelmsen Groups worldwide operations, the companies have an urgent need to exchange personal data between group entities. In certain jurisdictions the law prevents international transfers without adequate safeguards in place. This Agreement is designed to provide "adequate safeguards" and enable lawful international transfers of personal data by making the Binding Corporate Rules contractually binding and ensure individuals that their data is protected no matter where (which country) in the group their data is processed, and that an individual data subject may exercise his or her third party beneficiary rights.

### 2. DEFINITIONS

'**Agreement'** means this agreement;

**'HQ'** means 'Party 1', the company Wallenius Wilhelmsen ASA, Norway, Company number: 995 216 604;

**'Subsidiary Company'** means 'Party 2' of this Agreement;

'**WW-Group'** means the global group of entities which is under control by HQ;

'**Bound company**' means a WW-Group entity bound by the Binding Corporate Rules by the means of an Intra-Group Agreement;

**'Entity'** means any company within the WW-Group;

**'EU'** means the European Union;

**'CJEU'** means the Court of Justice of the European Union;

**'GDPR'** means the English version of the European Union General Data Protection Regulation;

**'EU/EEA'** means the European Union or European Economic Area, including Switzerland;

**'Safe country'** means any country with adequate personal data protection safeguards according to EU 'Working Party 29' or its successor from 25 May 2018, the 'European Data Protection Board';

**'Third-country'** means any country without adequate personal data protection safeguards according to EU 'Working Party 29' or its successor from 25 May 2018, the 'European Data Protection Board';

**'Binding Corporate Rules'** means the official document 'Binding Corporate Rules / Global Privacy Policy' in the version that was binding at the relevant date;

**'Legal & Compliance'** means the HQ legal department;

**'Appointed DPO'** means the Data Protection Officer at HQ Legal & Compliance; and

Other definitions, or if in doubt, shall be interpreted as of the EU GDPR Article 4.

**3. THE DUTIES**

3.1 The HQ agrees to:

a) Take responsibility for breaches of the Binding Corporate Rules as if Subsidiary Company was HQ.
b) Giving relevant EU/EEA supervisory authorities and relevant EU/EEA courts, including the CJEU, investigative and corrective powers.
c) Accept liability for Subsidiary Company's breaches. The HQ can be exempt from this liability in whole or in part, only if HQ prove that the Subsidiary Company was not responsible for the event giving rise to the damage.
d) Keep the Subsidiary Company informed and support it regarding all matters affected by the BCR.

3.2 The Subsidiary Company agrees to:

a) Respect any changes to the BCR without renewing this Agreement.
b) Respect any changes to this Agreement without re-signing this Agreement.
c) Authorize HQ through its appointed DPO or Head of Legal to enter into, inspect, amend or terminate agreements on behalf of the Subsidiary Company if they contain terms and conditions regarding personal data.
d) Respect 3.2c) by allowing signings as "Wallenius Wilhelmsen DPO on behalf of Subsidiary Company" or signing the agreements in Subsidiary Company's name following the WW Group DPO:s instructions.
e) Provide full support including personnel or managers to enforce compliance with the Binding Corporate Rules.
f) Allow WW Group DPO (with or without assistance) to enter into IT-systems, physical files or any other storage for personal data to assess compliance and fulfil the DPO tasks in the BCR section 12.
g) Co-operate with the competent European supervisory authority regarding the provisions and rights in the Binding Corporate Rules.

**4. COMPLIANCE**

4.1 Subsidiary Company warrants that it will:

a) Comply with the Binding Corporate Rules, including the related Global Policies.
b) Provide adequate safeguards according to the BCR regarding transfers of personal data to external companies using GDPR-compliant Data Processing Agreements.
c) Provide the WW Group DPO with copies of such signed agreements.
d) It will enforce the Binding Corporate Rules upon its employees by abiding the internal employee sanction policy "Global Employee Data Privacy Policy" (sanction policy) or a local policy with the same effect.
e) Provide data subjects with a link to the www.walleniuswilhelmsen.com/privacypolicy at their separate webpage (if existing) to allow data subjects access to the BCR including this Agreement.

**5. THIRD PARTY BENEFICIARY RIGHTS**

5.1 A data subject may enforce its individual third-party beneficiary rights in the BCR according to this Agreement if 5.1 a-c) is fulfilled:

a) the personal data regards him or her-self,
b) there would have been a breach of the GDPR if the breach was committed in the EU,
c) a bound WW Group company is responsible for the breach, either as a data owner or a data processor

5.2 The following rights is available for third party beneficiaries fulfilling 5.1 of this Agreement:

a) Right with respect to transparency, fairness and lawfulness;
b) Right to obtain a copy of the BCRs upon request;
c) Right to purpose limitation;
d) Right to data minimization and accuracy;
e) Right to limited storage periods;
f) Right with respect to special categories of personal data;
g) Right with respect to security and confidentiality, including the obligation to enter into contracts with all processors and the WW Group's obligation regarding personal data breach;
h) Rights pertaining to restriction on onward transfers to third parties not part of the WW Group;

i) Rights of access, rectification, erasure, restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling, and right to data portability;
j) Right to complaint through the WW Group's internal complaint mechanism;
k) Rights relating to national legislation preventing the WW Group from complying with the BCRs;
l) Rights related to the WW Group's cooperation duties with the Supervisory Authority; and
m) The right to receive compensation in the event of the Group's infringement of the BCRs.

5.3 A third party beneficiary may exercise his or her rights by:
a) Making an internal complaint by contacting the WW Group appointed DPO;
b) Using his or her right to report to a competent supervisory authority in EU/EEA; and
c) Using his or her right to judicial remedies, including the CJEU, according to the BCR.

**6. TERMINATION**

6.1 This Agreement will terminate immediately if the Subsidiary Company no longer is part of the WW Group. The third-party beneficiary rights remain intact if breaches of the BCR occurred before termination.

6.2 HQ may at all times terminate this Agreement if the Subsidiary Company stop processing personal data within BCR scope.