Binding Corporate Rules for Roust Group

Version: 1.0

Date: 25 May 2018

Table of Contents

1. Introduction

1. The objectives of the Binding Corporate Rules (the "BCR") are to provide adequate protection for the transfers and processing of Personal data by Roust Corporation and its affiliates engaged in a joint economic activity ("Roust Group").

2. All companies within Roust Group express their commitment to comply with the BCR.

3. The BCR introduces an obligation for all the companies of Roust Group and for all employees of Roust Group to respect the rules stated in the BCR.

2. Definitions

The following definitions apply to the BCR:

1. "Personal data" means any information relating to an identified or identifiable natural person;

   NOTE: 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.

2. "Processing" means any operation or set of operations which is performed on the Personal data or on sets of the 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;

3. "Controller" means an entity which determines the purposes and means of the Processing of the Personal data;

4. "Processor" means an entity which processes the Personal data on behalf of the Controller;

5. "Data exporter" is an entity (external , or internal within the group) which provides data for the Processing;

6. "Data importer" or 'recipient' is an entity (external , or internal within the group) which uses data for the Processing;

7. "Binding Corporate Rules or BCR" means the Personal data protection policies which are adhered to by the Controller or the Processor;

8. "BCR member" means any company operating within Roust Group as a Data exporter or Data Importer which is involved in intra-group transfers of the Personal data from and to the EU;

9. ”Supervisory Authority” means an independent public authority which is established by a Member State to be responsible for monitoring the application of the GDPR;

10. competent Supervisory Authority” means chosen Supervisory Authority to whom the application of BCR is submitted, established on the territory of a Member State for transfers or a set of transfers of the Personal data to the Controller or the Processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

11. ”“Member State” means a country within the European Union;

3. Scope and applicability

1. The scope of BCR is limited only to transfer and the Processing of the Personal data which can include data flows from and to the EU located BCR member operating within Roust Group. BCR members are listed in Annex A.

2. Any Processing or transfer of Personal data which is done internally by the BCR members are subject to local policies approved by the management of relevant company. Such policies impose on both the management and the employees the responsibilities for protection of the Personal data and sanctions for non-compliance with the policy.

3. The BCR are applied to the following types of data, reported or submitted for the corporate operation purposes:

- Employee Recruitment (above certain management level);
- Employee performance management and professional development;
- Payroll and administration of employee benefits (above certain management level);
- Corporate Finance;
- Database management;
- Training of employees and contractor representatives;
- Sales management or involving data of individuals (eg. Detailed daily reports on sales);
- Maintaining and building upon customer relationships, including claims and settlements;
- Marketing management or involving data of individuals (eg. Detailed reports on marketing events);
- Supply chain: invoices authorization;
- Supply chain: CAPEX authorization;
- Safety Alarms with regard to EHS area;
- Information necessary for fraud prevention or investigation, or other risk management purposes;

Description of the data flows between countries is presented in Annex B.

4. Additionally, the Personal data is processing horizontally by all BCR members for the identification management of employees and contractor representatives, and information verification services in Roust Group IT systems (eg. Helpdesk).

4. Data Subject rights

1. All BCR members ensure they follow fundamental rights of any Data Subject. It includes all of the following:

    a. The Personal data will be transferred and processed for specific, non-excessive and legitimate purposes. The Data Subject is given sufficient information in a clear and comprehensive way (usually by means of a fair Processing statement) about the uses and disclosures made of their data (including the secondary uses and disclosures of the data), the recipients or categories of recipients of the Personal data and the identity of the data Controller when such data is obtained by the BCR member.

    b. The Personal data is accurate and kept up-to-date. Any BCR member actively encourages Data Subjects to inform respective Data Controller when their Personal data changes.

    c. The Personal data will be kept as long as necessary. The Personal data will always be retained and/or deleted to the extent required by law, regulation and professional standards and in line with the applicable to local retention policies applying to the BCR member. When the retention period expires the BCR Member will dispose of Personal data only in a secure manner in accordance with appropriate local security policy.

    d. Personal data will be collected or processed at minimum level to fulfill the purpose of the Processing.

    e. Sensitive data[1] will be only used if it is absolutely necessary. If it would be the case an access to a sensitive personal data will be limited to appropriate persons (by either masking or making anonymous the data, where appropriate).

    f. The Personal data will not be transferred to external third parties without ensuring adequate protection for the data.

2. The Data Subject is granted the right of access, rectification, erasure, restriction, objection to the Processing. The above listed rights shall not be subject to decisions based solely on automated processing, including

[1] Sensitive data is data relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, criminal convictions, social security files, government identification numbers or financial account numbers.

profiling. The procedure for granting access is described in Annex C.

3. The Data Subject is given the right to complain through the internal compliant mechanism of any BCR member. Moreover, the Data Subject is free to lodge a complaint before competent Supervisory Authority with regards to the Data Subject habitual residence, place of work or place of alleged infringement or before the court of the EU Member state of his choice. The procedure for handling complaints is described in details in Annex D.

4. In case of potential or actual Personal data breach any relevant BCR member is obliged to follow the procedure as stated in this BCR, Annex E, and co-operate to the largest extent with Supervisory Authority concerned.

5. The Data Subject is given the right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of the BCR as stated in section 4, clause 1 (a-f) above.

5. Transparency and information rights

1. Before their data is processed the Data Subjects are given the following information:
    a. The identity of the Controller(s) and of his representative, if any;
    b. The purposes of the Processing for which the data are intended;
    c. Any further information such as:
    i) the recipients or categories of recipients of the data,
    ii) the existence of the right of access to and the right to rectify the data related exclusively to this particular data subject,
    iii) conditions under the data subject's request for abandoning or blocking the Processing could be granted, including erasing the data, if necessary,
    iv) compliant handling procedures (both, for the Data Subjects from whom data is collected directly, and third-party beneficiaries eg. customers of the Data exporter).

2. Every Data Subject has the right to have an easy access to his data.

3. Every BCR member collects, transfers and processes the Personal data only for explicit and legitimate purposes as set out in the BCR. In case the Personal data is obtained from third parties (including the BCR member customers) and publicly available sources, always reliable and reputable sources are used.

4. The BCR member transfers the Personal data only when:

    a. all applicable legal requirements are met;

b. the transfer is based on a clear business need;

c. the Data importer has implemented appropriate security measures;

5. The BCR member shall not disclose the Personal data except as set out in the BCR, its policies or as required or otherwise permitted by contract or applicable law.

6. Organization of data protection

1. Security and Compliance Director at CEDC International sp. z o.o. (the BCR member in Poland) is nominated as a Chief Data Protection Officer (the "CDPO" or the "Chief DPO").

2. Responsibilities of the CDPO include:

   a. overall supervision of the BCR execution;

   b. advise and support the Board of Directors of Roust Corporation with respect to all BCR aspects;

   c. monitoring and reporting on compliance at the corporate level;

   d. support of local DPOs and co-operation in handling incidents related to the BCRs' scope;

   e. dealing with Supervisory Authorities investigations;

3. The CDPO reports directly to Roust Corporation Board of Directors.

4. The BCR member can nominate it's local Data Protection Officer (the "DPO"). If such a role is not assigned to any person, designated manager will accept the Data Protection Officer tasks. List of designated persons per country is kept by the Chief DPO.

5. Responsibilities of the DPO include:

   a. monitoring data protection processing and transfers within the scope of BCR at local level;

   b. performing audits according to the BCR audit program;

   c. handling local complaints from the Data Subjects within the scope of the BCR;

   d. handling incidents related to the scope of the BCR at local level and cooperate with other DPOs and the Chief DPO, where relevant;

   e. reporting major privacy issues to the CDPO;

f. organizing and monitoring trainings at a local level;

g. assisting relevant Supervisory Authority in their audits or investigations, and implementing advices or recommendations of this Supervisory Authority.

7. Security measures and their effectiveness

1. The BCR member employs appropriate technical, organizational, administrative and physical security measures to protect the Personal data against unauthorized or unlawful Processing and against accidental loss or destruction.

2. Every trans-border transfer of the Personal data among the BCR members is protected by appropriate cryptographic techniques ensuring data confidentiality.

3. Only duly authorized personnel is allowed to be involved in the Personal data exchange among the BCR members.

4. The responsibility for monitoring, regular review, and improvement of its security system, policies and procedures to take into account emerging threats, as well as emerging technological safeguards and precautions is assigned to relevant IT departments.

5. When the Processing of the Personal data is outsourced by the BCR member to a third party, this BCR member will select reliable third parties that have implemented appropriate security measures. In particular, such third party will have the duty to notify without undue delay any Personal data breaches to the EU BCR member and to the relevant Data Protection Officer, and the Data Subjects where the Personal data breach is likely to result in a high risk to their rights and freedoms.

6. Any Personal data breaches related to the BCR (ie. the facts relating to the Personal data breach, its effects and the remedial action taken) will be documented, and the documentation will be made available to the Supervisory Authority.

7. Appropriate training on the BCR will be provided to personnel that have permanent or regular access to the Personal data, who are involved in the collection of data or in the development of tools used to process the Personal data.

8. All aspects of the BCR including methods of ensuring that corrective actions will take place are subject to audits performed on regular base.

9. Overall audit program for the BCR is prepared by the Chief Data Protection Officer and executed upon the approval of Roust Corporation Board of Directors.

10. Results of all audits will be communicated to the Chief Data Protection Officer.

11. Chief Data Protection Officer, or appropriate local Data Protection Officer, ensures that relevant Supervisory Authorities can have access to the results of the audit upon request and assists the Supervisory Authority in carrying out a data protection audit of any BCR member, if required.

8. Accountability and compliance

1. Every BCR member acting as data Controller will be responsible for and able to demonstrate compliance with the BCR.

2. In order to demonstrate compliance the EU BCR members will maintain a record of all categories of processing activities carried out in line with the requirements as set out in the GDPR. This record will be made available to relevant Supervisory Authority on request.

3. Appropriate technical and organizational measures will be implemented to ensure the leading data protection principles ie. privacy by design and privacy by default will be respected.

4. Impact assessment on data protection will be carried out if specific criteria as set up in the GDPR are met.

9. Applicable Law and liability

1. The BCR is compliant with relevant EU legislation, in particular with the General Data Protection Regulation (the "GDPR"), and local legislations in respective countries where companies of the Roust Group operate in.

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR)
- Privacy Act (R.S.C., 1985, c. P-21) (Canada)
- The Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada)
- THE DRAFT ACT AMENDING THE HUNGARIAN LAWS ON DATA PROTECTION (Hungary)
- Draft Personal data protection act (Poland)
- Federal Law of 27 July 2006 N 152-FZ ON PERSONAL DATA (Russia)
- Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions (Russia)
- Law on personal data protection (Відомості Верховної Ради України

(ВВР), 2010, № 34, ст. 481) (Ukraine)

- Decree on the coordination of materials of documents in the field of protection of personal data, НАКАЗ 08.01.2014 № 1/02-14 (Ukraine)

2. Where the local legislation requires a higher level of protection for the Personal data it will take precedence over the BCR.

3. Every EU BCR member exporting data out of the EU on the basis of the BCR will be liable for any breaches of the BCRs by the BCR member established outside the EU which received the data from this BCR member.

4. The BCR member that has accepted liability will also have the burden of proof to demonstrate that the BCR member outside the EU is not liable for any violation of the rules which has resulted in the Data Subject claiming damages. In that case the BCR member may discharge itself from any responsibility.

10. Exemptions from respecting the BCR

1. In case a BCR member has reasons to believe that the legislation applicable to him prevents the company from fulfilling its obligations under the BCR, or has substantial effect on the guarantees provided by the rules, he will promptly inform the Chief Data Protection Officer and relevant Data Protection Officer, except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

2. Furthermore, where any legal requirement a BCR member is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by the BCR, the problem should be reported to relevant Supervisory Authority. This includes any legally binding request for disclosure of the Personal data by a law enforcement authority or state security body. In such a case, the Supervisory Authority will be clearly informed about the request including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

3. If in specific cases such suspension or notification are prohibited by law then the BCR member concerned will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

4. If, in the all above cases, the requested BCR member is not in a position to notify relevant Supervisory Authority then it is obliged to provide general information on annual basis on the request of the Supervisory Authority (e.g. number of applications for disclosure, type of data requested, requester, if possible).

5. In any case the transfers of the Personal data by a BCR member any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

11. Updating the BCR

1. The BCR will be modified if at least one of the following conditions takes place:

– any significant changes are needed to the BCR itself,

– modifications of the regulatory environment in terms of rights and obligations of the Supervisory Authorities,

– changes to the company or corporation structures resulting in a new authorizations/ approval from the Supervisory Authority.

2. Where a modification would possibly affect the level of protection offered by the BCR or significantly affect the BCR (i.e. changes to the binding character), it must be promptly communicated to the relevant Supervisory Authorities, via the competent Supervisory Authority.

3. Upon approval of the Board of Directors of Roust Corporation the Chief Data Protection Officer has a duty to report changes without undue delay to all BCR members and to the relevant Supervisory Authorities via the competent Supervisory Authority.

4. The following changes of BCR do not cause re-applying for the approval from the competent Supervisory Authority:

– the Chief Data Protection Officer keeps a fully updated list of the BCR members and keeps track of and record any updates to the rules and provides the Data Subjects or Supervisory Authorities with the necessary information upon request;

– no transfer is made to a new BCR member until the new BCR member is effectively bound by the BCRs and is able to demonstrate compliance;

– any changes to the BCRs or to the list of BCR members are reported once a year to the relevant Supervisory Authority, via the competent Supervisory Authority, with a brief explanation of the reasons justifying the update.

Annex A List of BCR members

Roust Corporation	CEDC International sp. z o.o
232 Madison Avenue, Suite 1600, NY 10016 New York, USA	ul. Kowanowska 48, 64-600 Oborniki, Poland
PWW sp. z o. o.	B2B Wine &Spirits sp. z o.o.
ul. Bobrowiecka 8, 00-728 Warszawa, Poland	Lubińska 10, 05-532 Lubna, Poland
ROUST Hungary Kft.	ROUST UKRAINE LLC
Alkotás u. 50 1123 Budapest, Hungary	Konstantinovskaya str, 2A, 04071, Kiev, Ukraine
JSC «Roust Russia»	"Parliament Production", LLC
Eniseiskaya str., b. 1, con.1, 129344, Moscow, Russian Federation	Balashiha, microregion Saltikovka, Popovka str., ownership 5, 143916, Moscow region, Russian Federation
"Russian Standard Vodka" LLC	Bravo Premium LLC
Pulkovskoe shosse 46, build 2, 196140, Saint-Petersbourg, Russian Federation	Kuznetsovskaya str., b. 52, con.3, letter A, 196105, Saint-Petersbourg, Russian Federation
CJSC "ROUST INC."	Roust Distribution Limited
Shoushari village, Pulkovskoe road, b.52, letter A, 196140, Saint-Petersbourg, Russian Federation	Diagorou 4, Kermia, Building, 6th floor, Office 601, Nicosia, P.C. 1097, Cyprus
Roust Distribution (UK establishment of ROUST DISTRIBUTION LIMITED)	Russian Standard Vodka (USA), Inc.
Thomas House, 84 Eccleston Square, London, United Kingdom, SW1V 1PX	c/o Corporation Service Company, 2711 Centerville Road, Suite 400, in the City of Wilmington, County of New Castle, Delaware, USA
JOINT STOCK COMPANY "DISTILLERY TOPAZ"	"Trading House "Russian Alcohol – Moscow" LLC
46, Oktyabrskaya str., Pushkin, Moscow region, 141200, Russian Federation	1/1, Eniseyskaya str., Moscow, 129344, Russian Federation
Russian Standard Vodka Canada Ltd.	F.lli Gancia & c. spa
Suite 4000, Bay street, 199, Toronto, Ontario, Canada, M5L 1A9	Corso liberta 66, 14053 Canelli, Asti, Italy

Annex B Description of data flows

Presentation of data flows for relevant trans-border exchange between BCR members (per country)

Type of data, **transferred or reported** to Corporate HQ or being subject to intra-group exchange*, which **could** involve personal data	Companies per country							Remarks per specific country
	Russia	Poland	Ukraine	UK/Cyprus	USA/Canada	Hungary	Italy	
Employee Recruitment - above certain management level	no	yes	yes	yes	yes	yes	no	
Employee performance management and professional development;	no	no	yes	no	yes	yes	yes	
Payroll and administration of employee benefits - above certain management level;	yes	yes	yes	yes	yes	yes	yes	
Corporate Finance;	yes	yes	yes	no	yes	yes	yes	
Database management;	no	no	no	yes	not relevant	yes	yes	Hungary: owner of the Hungarian legal entity is CEDC, hence such and similar data can be shared with CEDC
Training of employees and contractor representatives;	no	no	yes	no	no	no	no	
Sales management or involving data of individuals (eg. Detailed daily reports on sales);	no	yes	yes	no	no	no	no	Hungary: such data is being reported, but does not show data at individual sales person level
Maintaining and building upon customer relationships, including claims and settlements;	no	no	yes	no	not relevant	no	no	
Marketing management or involving data of individuals (eg. Detailed reports on marketing events);	not relevant	no	no	no	yes	no	no	US - for promo models, personal names are on invoicing
Supply chain: invoices authorization;	no	yes	yes	no	no	no	not relevant	
Supply chain: CAPEX authorization;	no	yes	yes	no	no	yes	no	
Safety Alarms in with regard to EHS area;	no	yes	yes	not relevant	not relevant	no	not relevant	
Neccessary for fraud prevention or investigation, or other risk management purposes;	no	no	yes	no	yes	no	no	US - for investigation of credit card fraud, information was provided to auditor
For identification (identity management for employees and contractor representatives) and information verification purposes (eg. Helpdesk);	yes	yes	yes	no	yes	yes	yes	
*between all or some of companies in the Roust Corporation								

Answer		**what it means**
yes		reports can include personal data (eg.of employees or customers)
no		reports are aggregated and do not include personal data
not relevant		such type of data are not processed in relevant chapter

Annex C Data Subject access request procedure

Introduction

EU Data Protection law gives individuals whose Personal data is collected and/or transferred at the EU territory the right to be informed whether any Personal data about them is being processed by an organization. According to the GDPR, art.15, the Data Subject has a right to access to the following information:

(a) the purposes of the Processing;

(b) the categories of Personal data concerned;

(c) the recipients or categories of recipient to whom the Personal data have been or will be disclosed, in particular recipients in third countries or international organizations;

(d) where possible, the envisaged period for which the Personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the Controller rectification or erasure of Personal data or restriction of Processing of Personal data concerning the data subject or to object to such Processing;

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

(g) where the Personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the data subject.

Additionally, where Personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards.

All Data Subjects whose Personal data is collected and used at the EU territory **and additionally,** transferred between the BCR members will benefit from the right of access in accordance with the terms of this procedure. Where the applicable non-EU data protection law differs from any aspect of the procedure, this local data protection law will prevail.

General provisions

1. The request must be made in writing, which can include e-mail.
2. The procedure deals with the Data Subject access requests which refer to the BCR scope (valid request).
3. Any BCR member is not obliged to comply with a request unless the Data Subject who submits this request provides reasonable confirmation of his/her identity.
4. The BCR member shall respond to a valid request within 30 calendar days (or any shorter period as may be stipulated under local law) of receipt of

that request.

5. Under normal circumstances no fee will be applied but this will be left to the discretion of the BCR member to which the request is made and in accordance with local applicable law.

Receiving and accepting the request

6. If any employee, partner or subcontractor of the BCR member receives any request from an individual for granting access to their Personal data such communication shall be passed immediately to relevant local DPO together with the date of receipt and any other information which may assist the DPO to deal with the request.
7. The local DPO makes an initial assessment of the request to decide whether it is a valid request.
8. The local DPO contacts the individual in writing to fulfill at least one of the following:
    a. Confirming receipt of the request for further Processing,
    b. Asking for additional information, including confirmation of identity,
    c. Declining the request claiming it is not valid one.
9. Following 8.c. the grounds for declining the request can be at least one of the following:
    a. Where the request is made to the BCR member and relates to the use or collection of the Personal data by that BCR member, and the refusal to provide the information is consistent with the data protection law within relevant jurisdiction;
    b. In the opinion of the BCR member:
        i. compliance with the request would prejudice the essential business interests of the BCR member (which includes management planning, corporate finance or negotiations with the Data Subject who submits the request);
        ii. it is necessary to do so due to public security, defense, national security and the activities of the state in areas of criminal law;
        iii. it is necessary for the protection of the data subject himself/herself, or of the rights and freedoms of others;
    c. If the Personal data is held by the BCR member in non-automated form and is not or will not become part of a filing system;
    d. Where the provision of the Personal data requires the BCR member to use disproportionate effort.
10. The local DPO can refer any complex cases to the Chief DPO for advice, particularly where the request includes information relating to third parties or where the release of Personal data can prejudice business confidentiality or legal proceedings.

Search and response

11. The local DPO arranges a search of all relevant electronic and paper filing systems.
12. The information requested is transformed by the local DPO into a readily understandable format (eg. internal codes or identification numbers that correspond to Personal data shall be removed before sending to the Data Subject). Then the local DPO sends to the Data Subject all information required to be provided in response to the request.
13. Where the provision of the information in permanent form is not possible or would involve disproportionate effort there is no obligation to provide a permanent copy of the information. In such circumstances the individual may be offered the opportunity to have access to the information by inspection, or remote access to the database, or to receive the information in another form.

Requests for erasure, amendment or cessation of processing of information

14. If the request is received for the deletion of that individual's Personal data, such request must be considered and dealt with as appropriate by the local DPO. If the Processing is based on other compelling legitimate grounds, such request is declined.
15. If the request for a change in that individual's Personal data is received, such information must be rectified or updated accordingly if there is a legitimate basis for doing so.
16. If the request is to cease Processing that individuals' Personal data because the rights and freedoms of the individual are prejudiced by virtue of such Processing by the BCR member, the matter is to be referred by the local DPO to the Chief DPO for further assessment. Where the Processing undertaken by the BCR member is indispensable on any legitimate ground, the request is declined.

Annex D Procedure for handling complaints

Introduction

If the Data Subject considers that his/her Personal data has been processed in violation of the BCR, this individual may report concerns to any BCR member in written, via email, or as otherwise indicated in the BCR using contact details given in Annex A to BCR.

The purpose of this procedure is to explain how complaints brought by an individual whose Personal data is processed by the BCR member, and within the scope of BCR, are dealt with.

Processing the compliant

1. If any employee, partner or subcontractor of the BCR member receives any complaint in relation to the BCR such communication shall be passed immediately to relevant local DPO together with the date of receipt and any other information which may assist the DPO to deal with the complaint.
2. The local DPO acknowledge receipt of a complaint to the individual concerned within 5 working days.
3. The local DPO is handling the complaint with support from relevant business or other organizational units, and from the Chief DPO, if necessary.
4. In normal circumstances the local DPO is preparing a response to the individual within 30 days. If the response cannot be given within this period due to the complexity of the complaint, the local DPO informs the individual accordingly, and provide a reasonable estimation of time when the response is provided. In any circumstance this timeframe may not exceed six months from the date the complaint has been submitted.

Resolving disputes

5. If the individual questions the response, or any aspect of the local DPO findings, the matter is referred to the Chief DPO who reviews the case, and decides either decision either to keep the original response or to substitute a new one.
6. The Chief DPO takes every reasonable step to resolve the dispute.
7. The Chief DPO action may not exceed 60 days from the date of re-submission of the complaint.

Final provisions

Regardless the procedure described above an individual whose Personal data is collected and/or used has the right to lodge a complaint with a single Supervisory Authority, in particular in the Member State of his or her habitual residence, or employment, and the right to an effective judicial remedy in accordance with the provisions of the GDPR, and this includes where they are not satisfied with the way in which the complaint relating to the BCR has been resolved.

Individuals entitled to such rights will be notified accordingly as part of the complaint handling procedure.

Annex E Incident handling procedure

Introduction

A personal data breach (called hereinafter an incident) can happen for a number of reasons, for example:

- loss or theft of data or equipment on which data is stored, or through which it can be accessed;
- loss or theft of paper files;
- unauthorized access to data (eg. as a result of hacking attack);
- inappropriate access controls allowing unauthorized/unnecessary access to data;
- equipment failure ;
- administrator or user error;
- unforeseen circumstances such as a fire or flood;

The General Data Protection Regulation states as soon as the Controller (within the scope of BCR – the BCR member concerned) becomes aware that the Personal data breach has occurred, such incident should be reported to relevant Supervisory Authority without undue delay and, where feasible, not later than 72 hours after information on the incident has been confirmed, unless the EU BCR member concerned is able to demonstrate, in accordance with the accountability principle, that the Personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Reporting an incident

1. If the Personal data breach is identified or suspected it is immediately reported to the local DPO.
2. In order to improve overall understanding of the risks to Personal data and address them before breaches occur any employee, partner or subcontractor is encouraged to report 'near misses' (ie. incidents which have almost resulted in a data breach except for an early intervention or simply 'luck').

Investigating the incident

3. Local DPO performs first assessment of the incident.
4. If trans-border exchange of Personal data is affected the local DPO informs without undue delay the DPO(s) from relevant BCR member(s), and the Chief DPO. The team of DPOs work is coordinated by the local DPO from the EU BCR member concerned, or Chief DPO, where relevant.
5. The team of DPOs from relevant BCR members analyses further the case, and decide whether any immediate corrective/containment/escalation actions are required.
6. Depending on the type and severity of the incident and upon the decision of the team of DPOs from relevant BCR members the local DPO or Chief PO,

whoever is designated as the coordinator of the team:

- Updates the Personal data breach log, and close the log if the incident does not require further assessments; or
- Opens an investigation and appoints an appropriate investigation team consisting of relevant internal or external experts (eg. from IT unit from the BCR member(s) concerned);
- Monitors the activity of investigation team and performs ongoing assessment of the incident.

7. The investigation results in the following:
    - Determining the nature and the extent of the incident, the type and volume of data involved and the identity of the Data Subjects ;
    - Performing a risk assessment to the rights and freedoms of the Data Subjects;
    - Identifying actions relevant BCR member(s) needs to take to contain the breach and recover information;
    - Recommending actions required to prevent a recurrence of the incident in the future.
8. In case the ongoing assessments show the incident cannot be contained in due time the Chief DPO, and the management of the EU BCR member(s) concerned are informed.
9. Based on the investigation results the local DPO or Chief DPO, where relevant, completes a full ex-post breach report and updates the Personal data breach log.

Reporting Breach to relevant Supervisory Authority or Data Subject(s)

10. If the risk assessment to the rights and freedoms of the Data Subjects is shown to be high the local DPO from the EU BCR member concerned, or Chief DPO, where relevant, coordinate the incident reporting to relevant Supervisory Authority. The management of the BCR member(s) concerned, or the Corporate Management, where appropriate, is informed as well.
11. Further, if this is determined to be the case the incident is reported to the Data Subjects without undue delay. Such information campaign is coordinated by the local DPO from the EU BCR member concerned, or Chief DPO, where appropriate, with the support of relevant legal and/or PR units.

Post incident activities

After closing the incident, the Personal data breach log or the ex-post breach report is examined by the Chief DPO to determine whether any update to the BCR is required. The Chief DPO co-ordinates any training and communications messages from the lessons learnt.