Personal Data Protection Policy
C6.PLC.01

Version 1.0
25 April 2018

Legal notices

Summary

NAME	Personal Data Protection Policy
ID	C6.PLC.01
PROCESS SUPERVISOR	A.A. Ilyin, Chief Financial Officer, EuroChem Group
PROCESS OWNER	V.V. Sidnev, General Counsel, EuroChem Group
DEVELOPED BY	E.V. Kholmanskikh, Chief Compliance Officer, EuroChem Group
VERSION	1.0
EFFECTIVE DATE	25 April 2018
APPROVAL DATE	24 April 2018

Revision history

Version	Effective date	Purpose	Revision details
1.0	25 April 2018		N/A

Contents

1. Terms and definitions

Unless a contrary indication appears, words and expressions defined (or expressed to be subject to a particular construction) in the Code of Conduct and the Compliance Policy have the same meaning (or be subject to the same construction) in this Personal Data Protection Policy (the "Policy").

Additionally, the following definitions will apply:

Term	Definition
"Personal data"	means any information relating to an identified or identifiable Data subject; this is a very wide range of personal identifiers, including a natural person's name, (professional) telephone number, (professional) email address, identification number, location data, online identifier, etc.
"Sensitive data"	means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
"Data Contoller" or " Contoller"	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
"Data Processor" or "Processor"	means a natural or legal person which processes personal data on behalf of the Controller.
"Data subject"	means any living individual who is the subject of Personal Data held by the Group.
"Processing"	means any operation or set of operations which is performed on Personal Data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"Personal Data breach"	means a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
"Data subject consent"	means any freely given, specific, informed and unambiguous indication of the Data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.
"EU Data Protection Officer"	means an employee of the Group who is responsible for the Policy deployment within the EU part of the Group
"Global Data Protection Officer"	means an employee of the Group who is responsible for the Policy deployment within the Group
"Local Data Protection Officer"	means an employee of the Group who is responsible
"Data Processor agreement"	means an agreement concluded between the Group and any counterparty for the Policy deployment within the relevant Group.
"Retention Schedule"	means a special schedule in according with documents are kept within concrete timeline.

2. Application

2.1. Intended Use

In this Policy outlined the key principles of Personal Data Protection and Processing of Personal Data, applicable for the Group.

As an employer, customer and supplier each member of the Group collects and uses personal data pertaining to employees, business partners, customers, prospects, etc. While the handling of these personal data is indispensable to our operations, the Group realizes that protecting the personal rights and privacy of each individual is the foundation of trust in all relationships. This is why the Group wants to excel in the protection and correct Processing of Personal Data.

For the Group it's crucial to comply with Personal Data Protection requirements in the countries where the business is conducted and where Data subjects reside. All members of the Group have to comply with local regulations from around the world that govern the controlling and processing of personal data.

The top priority of the Group is to ensure universally applicable, worldwide standards for handling personal data. This Data Protection Policy is the general framework that applies across the Group. Given the variations in local regulations and diversity of activities, it is however inevitable that the implementation of these Data Protection principles might slightly vary for members of the Group.

This Policy shall be brought to the attention of all employees which shall comply with the Policy and perform its requirements. Furthermore, the Policy applies to counterparties who are dealing with any member of the Group and who have or may have access to Personal Data. These counterparties will be expected to have read, understood and comply with this Policy.

2.2. Area of application and mandatory legal requirements

The countries where the Group conducts business, can be divided into 3 big groups depending on the location: EU, Russia and other countries.

Except for the head offices in Switzerland and Russia, some members of the Group are located in the EU. EU Data Protection rules (Regulation (EU) 2016/679 (the General Data Protection Regulation or "GDPR") are stringent and apply on a harmonized basis across the whole of the EU. The scope of application of the GDPR is broader than just the EU, since it also applies to members of the Group established outside the EU if the Data subject is resident in the EU.

The Group has taken it upon itself to use the principles and obligations under the GDPR as the blueprint for its Data Protection Policy. However, separate members of the Group also need to comply with local regulations. This Data Protection Policy merely supplements the local Data Protection regulations. The relevant local regulation takes precedence in the event that it conflicts with this Data Protection Policy or has stricter requirements than this Data Protection Policy. Examples of local regulations which are relevant for some members of the Group include:

- Federal Law № 152-FZ on personal data of 2006 (applicable for Russia);
- Federal Act on Data Protection (FADP) of 19 June 1992 (applicable for Switzerland);
- Local legislation on corporate governance and data retention periods.

3. General provisions

3.1. Objectives of the Policy

The main objectives of the Policy are as follows:

- To protect freedoms and rights of all Data subjects and inform them on these;
- To Process Personal Data in a correct manner;
- To avoid any Personal Data breaches and security issues in general;
- To increase awareness of the Personal Data Protection regime in general.

3.2. Principles of the Policy

All processing of Personal Data must be conducted in accordance with the Data Protection principles as set out in the GDPR. The Group's policies and procedures are designed to ensure compliance with these principles.

In short, we, as the Group commit ourselves to compliance with the following principles:

- The fairness and lawfulness principle: we commit ourselves to only process personal data insofar as we have informed the Data subject and insofar as there is a legal basis for the processing.

- The purpose limitation principle: we will only process personal data for specified, explicit and legitimate purposes and will not further process these data in a manner that is incompatible with those purposes.

- The data minimization principle: we will only process the personal data that are adequate, relevant and limited to what is necessary in relation to the purposes for which these data are processed.

- The accuracy principle: we will only process data that are accurate and, where necessary, kept up to date. We will take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- The processing limitation principle: we will keep all personal data in a form that permits identification of Data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- The security principle: we will only process data in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using all appropriate technical or organizational measures.

- The accountability principle: we will be responsible for, and will at all times be able to demonstrate, compliance with the abovementioned Data Protection principles either towards the competent authorities or toward the Data subjects.

4. Data Protection measures

The Group's commitment to the implementation of the abovementioned Data Protection principles is illustrated by the following measures we have taken:

4.1. Lawful and fair processing

The Group ensures that data is collected and processed fairly and lawfully. We take all reasonable steps to ensure that personal data is up to date, accurate and only retained for a predefined period of time.

The Group ensures that, depending on the category the Data subject belongs to, the collected data will only be used on the hereafter described fair and lawful bases.

4.1.1. Employees' data

Employees' data means all data processed by any member of the Group related to the employees and (when required) their spouses. However employees' data is broader than just personal data of the current employees. There are also other categories of data related to employment, such as data on retired employees and applicants.

All employees' data are collected by the Group in which employee is employed. The employer is considered to be the Controller of the data (meaning that the Group determines the purposes and means of the processing of the data).

1. lawful basis for processing activities

In the employment relationship the vast majority of data processing activities is legitimized by the necessity of the performance of a contract: members of the Group wouldn't be able to properly execute its obligations under its employment contracts, without being able to process data of its employees.

Some of the data processing activities are legitimized by a legal obligation: in all countries where members of the Group conducting business, there is a legal obligation to process certain personal data of employees, e.g. for reasons of social security, insurances, payment of salaries, etc.

Some of the data processing activities might also be permitted under collective agreements. Collective agreements are pay scale agreements or agreements between employers and employee representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended data processing activity, and must be drawn up within the parameters of national Data Protection legislation.

Each member of the Group can in almost all instances also rely on legitimate interests to process personal data, since it is necessary for the proper functioning of its business (e.g. while a member of the Group does not have an employment contract with applicants, but the Group has a legitimate interest to assess potential candidates, especially when they initiate the application process by contacting the member of the Group).

In a very limited number of cases processing activities might need to be legitimized by express consent given by the employee (e.g.: publishing an interview or photograph in an internal journal, etc.).

Each member of the Group is solely responsible for identifying the lawful basis of the processing activities.

2. fair processing

A detailed overview of how the employees' data are processed, can be found in our more detailed policies. Here we only give a short overview of some aspects of the processing activity:

- Minimization: the Group ensures that the employees' data it processes are limited to a minimum.
- Accuracy: the Group ensures that all employees' data are regularly updated on an entity wide level and that each employee can at all times ask to correct any wrong data.
- Storage limitation: all employees' data will be processed during the duration of the employment contract. After termination of the employment contract a large part of the data will be deleted once the required detention period has been observed, unless otherwise required by law or the Data subject has explicitly agreed to remain on file for further specific processing activities.
- Security: All personal data are processed in a secure manner. E.g.: access to the data is restricted on a need-to-know basis, data of the Group often pseudonymizes data when transferred to a third party, etc.
- Processing of sensitive data: sensitive data, such as data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sexual life of the Data subject will be processed with the additional care required.
- The Group minimizes automatic processing of personal data. If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g. as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee.

Each member of the Group is solely responsible for the fair processing of the employees' data.

4.1.2.Counterparties' data

Counterparties' data means personal data on customers, subcontractors, suppliers, business partners, visitors of the website, etc. While this will always be professional data, meaning that almost no sensitive data will be processed, each email address or phone number will be considered to be personal data.

Insofar as the Group has collected the counterparties' data directly from the Data subject, it will function as Data Controller. The nature of the Group's business might necessitate that counterparties' data is collected from another party. In this case the Group will only be a Data Processor, not a Data Controller, unless otherwise agreed upon.

1. lawful basis for processing activities

In the contractual relationship the vast majority of data processing activities is legitimized by the necessity of the performance of a contract: the Group wouldn't be able to properly execute its obligations under its contracts, without being able to process the relevant data.

Some of the data processing activities are legitimized by a legal obligation: in some countries where the Group doing business , there is a legal obligation to process certain personal data by suppliers.

The Group can in almost all instances rely on legitimate interests to process personal data, since it is necessary for the proper functioning of its business.

In a very limited number of cases processing activities might need to be legitimized by express consent given by the third party (e.g.: receiving a newsletter of the Group, etc.).

Insofar as the Counterparties' data are controlled by the Group (meaning that a member of the Group determines the purposes and means of the processing of the data), this Group will be responsible for identifying the lawful basis of the processing activities.

2. fair processing

A detailed overview of how the counterparties' data are processed, can be found in our more detailed policies. Generally speaking, the same principles apply as those that apply to the processing of employees' data as described under 4.1.1.

Noteworthy are the following additional principles:

- In case the processing of counterparties' data is collected through the Group's website and online tools: if personal data is collected, processed and used on websites, the Data subjects will be informed of this in a privacy statement and, if applicable, information about cookies. The privacy statement and any cookie information will be integrated so that it is easy to identify, directly accessible and consistently available for the Data subjects.

  Insofar as we create user profiles (tracking) on our websites, the Data subjects will always be informed accordingly in the privacy statement. Personal tracking may only be effected if it is permitted under national law or upon consent of the Data subject.

  If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the Data subject will offer sufficient protection during access.

- Digital Marketing: the Group shall mainly carry out digital marketing strategies in a 'business to business' context, where there is no legal requirement to obtain consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

  However, as a general rule the Group will strive to always obtain consent before sending promotional or direct marketing material to a counterparty Data subject.

Insofar as the Group is the Controller of the counterparties' data, the Group will be responsible for identifying the lawful basis of the processing activities.

4.1.3.Consent

Insofar as the Group relies on consent as a lawful basis for processing, the following conditions will apply:

Declarations of consent will be submitted voluntarily, in writing and in compliance with local regulations. Any consent that does not meet these conditions, is void. The declaration of consent will be obtained in writing or electronically for the purposes of documentation. Before giving consent, the Data subject will be informed of the extent of the processing activities. The Data subject can withdraw their consent at any time.

For Sensitive data, explicit written consent of Data subjects must be obtained unless a clear alternative legitimate basis for processing exists.

In most instances, consent to process Personal and Sensitive data is obtained routinely by the Group using standard consent documents.

4.2. Protection of data subjects' rights

Each member of the Group ensures that the Data subject whose Personal Data is processed by the Group and can exercise the following individual rights.

- **The right to be informed:**

  The Policy provides a full overview of the general principles under which the Group processes Personal Data. It is shared with the Data subjects at the time their Personal Data is collected (insofar as the Group is the Controller) and is publicly available on www.eurochemgroup.ru.

  However, in case the Data subject explicitly requests this, the relevant member of the Group (meaning the Controller or Processor of the Personal data) will provide the Data subject with the information on its Personal Data in a concise, transparent, intelligible and easily accessible manner. The Group reserves the right to decline a request for information insofar as the Data subject already has the information or if it would involve a disproportionate effort to provide it.

  Upon request, The Group shall provide the following information: 1) the name and contact details of the entity, 2) the purposes of the processing, 3) the lawful basis for the processing; 4) the categories of Personal Data obtained; 5) the recipients or categories of recipients of the personal data, 6) the details of transfers of the Personal Data to any third countries or international organizations (if applicable), 7) the retention periods for the personal data, 8) the rights available to Data subjects in respect of the processing, 9) the right to withdraw consent (if applicable), 10) the right to lodge a complaint with a supervisory authority.

- **The right of access:**

  In order to ensure that Data subjects are aware of and can verify the lawfulness of the processing activities, the Group grants them the right to obtain confirmation that the Data subject's data is being processed; access to the personal data; and other needed supplementary information. The format of the access shall be mutually agreed.

- **The right to rectification:**

  In case a member of the Group processes inaccurate or incomplete personal data, the Data subject may ask to rectify, or complete the data. Hence the Group reserves the right to refuse a request for rectification when allowed by an applicable regulation.

- **The right to erasure and the right to restrict processing:**

  Data subjects have the right to have their Personal Data erased from the records of the Group, if 1) the Personal Data is no longer necessary for the purpose of original collection or processing it for; 2) a member of the Group is solely relying on consent as the lawful basis for holding the data, and the Data subject withdraws its consent; 3) a member of the Group is solely relying on legitimate interests as the basis for processing, the Data subject objects to the processing of their data, and there is no overriding legitimate interest to continue this processing; 4) a member of the

Group is processing the Personal Data for direct marketing purposes; 5) a member of the Group has processed the Personal Data unlawfully.

As an alternative to requesting the erasure of personal data, the Data subject can request a relevant member of the Group to restrict the processing of their Personal Data to storing the data, but not using it otherwise. Such a restriction can be requested if: 1) the Data subject contests the accuracy of their Personal Data and a member of the Group is meanwhile verifying the accuracy of the data; 2) the data has been unlawfully processed and the Data subject opposes erasure and requests restriction instead; 3) a member of the Group no longer needs the Personal Data but the Data subject needs the Personal Data to be kept in order to establish, exercise or defend a legal claim; 4) the Data subject has objected to a member of the Group processing the data and the member is meanwhile considering whether its legitimate grounds override those of the Data subject.

- **The right to data portability:**

  Under strict conditions, a Data subject may request a member of the Group to provide it with all its Personal Data in a structured, commonly used and machine readable form. This should allow the Data subject to transmit its data to another organization. If this is technically feasible the Data subject might request to transmit the data directly to this other organization.

  The right to data portability only applies: 1) to Personal Data an individual has provided to a Controller; 2) where the processing is based on the Data subject's consent or for the performance of a contract; and 3) when processing is carried out by automated means.

- **The right to object:**

  If a Data subject has an objection against the processing of its Personal Data on "grounds relating to his or her particular situation", the Data subject has the right to object to: 1) processing based on legitimate interests and 2) direct marketing (including profiling).

  In this case, a member of the Group will stop processing the Personal Data unless: 1) it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the Data subject; or 2) the processing is for the establishment, exercise or defense of legal claims.

All requests for the execution of the abovementioned rights, must be directed to the Data Protection Officer. Unless otherwise allowed under applicable regulation, each request must be done in writing.

Unless otherwise stipulated by an applicable regulation, a response to each request will be provided within 30 days of the receipt of the written request from the Data subject. Appropriate verification must confirm that the requestor is the Data subject or their authorized legal representative.

Unless otherwise stipulated by an applicable regulation, each request will be free of charge unless the request is deemed to be unnecessary or excessive in nature.

4.3. Security of Personal Data

The Group commits itself to comply with what is considered best industry practice regarding IT-security.

In addition to this, each Group Company has adopted physical, technical, and organizational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorized alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

While the security measures vary and depend on the member of the Group, the following measures will be considered to be the minimal safeguards:

All Personal Data are treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerized, password protected in line with corporate requirements; and/or
- stored on (removable) computer media which are encrypted.

Manual records may not be left where they can be accessed by unauthorized personnel and may not be removed from business premises without a special authorization. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

Personal Data may only be deleted or disposed of in line with the Retention Schedule.

The Group must ensure that Personal Data is not disclosed to unauthorized counterparties including family members, friends, government bodies unless required by laws. All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorized by the Data Protection Officer.

Each member of the Group ensures that all employees adhere to this Policy and the Codes of Conduct. Moreover each member of the Group guarantees that all employees responsible for the execution of the Policy will be properly trained, informed and supported (see also article 4.6)

4.4. Personal Data breaches

A Personal Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. It may occur by way of a technical or physical incident. Given that such breaches always come as a complete surprise, each member of the Group has taken all reasonable preparations to prevent that a personal data breach ends in a catastrophe.

Each member of the Group has robust breach detection, investigation and reporting procedures in place. These are described in the Group Company's data breach Policy. In addition each member of the Group maintains a data breach register, in which it maintains information on the facts relating to all personal data breaches, the effects of the breaches and the efforts and remedial actions taken.

While the policies of the different members might vary, each data breach procedure will contain the following steps:

- All employees must inform their supervisor immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data (Data Protection incidents). The supervisor will subsequently inform the Local Data Protection Officer, the EU Data Protection officer and the Global Data Protection Officer.

- The Data Protection Officers decide whether the Data Protection incident actually resulted in a breach of personal data. For instance, lost USB sticks, stolen laptops, malware infections or hacked databases containing personal data are considered personal data breaches. A threat or a shortcoming in security measures, such as weak passwords or outdated firewalls, are not considered a personal data breach as long as no personal data has been leaked.

- If the Data Protection incident is indeed a breach of personal data, the Data Protection Officers will investigate the scope of the breach. They will investigate the scope of the personal data breach, how many data subjects might be affected, whether the breach might result in a risk to the freedoms and rights of the data subjects, whether the compromised personal data contain Sensitive data, whether the compromised data was secured (encrypted or otherwise), whether other parties might be involved in the data breach and which steps should be taken to mitigate (further) loss of the Personal data.

- Based on the above assessment, the Data Protection officers will decide whether the relevant supervisory authority and the Data Subject must be informed of the breach. The notification to the supervisory authority is not necessary if the Personal Data breach is unlikely to result in a risk to the rights and freedoms of individuals.

- Should a notification of the personal data breach be required, then the Group will notify the competent supervisory authority and provide them with all required information within 72 hours after having become aware of it.

- Where a personal data breach is likely to result in a ''high risk'' to the rights and freedoms of individuals, the Group will notify those concerned directly. A ''high risk'' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority. If individual notifications would be a disproportionate effort, the Group can use some form of public communication instead provided that this will be equally effective in informing individuals.

- To maintain the high level of visibility and transparency each member of the Group will document all Data Protection incidents (whether reported or not), including the facts related to the breach, its effects and actions taken or planned. All this documentation shall be enable for the Supervisory Authority in order to verify compliance with the notification obligations. All facts of data breach should be accumulated in a special template “A Data Breach Register” (Annex 2).

4.5. Retention and disposal of data

As already discussed under article 4.1 of this Policy, Personal Data cannot be processed longer that is needed for the purpose of its processing.

Each member of the Group has defined and set up a separate Retention Schedule in accordance with Annex 3. The retention periods are based on local legislation requirements for different types of Personal Data categories. Usually the local legislation categorizes the personal data as follows:

1. Accounting and Finance
2. Contracts
3. Corporate records
4. Correspondence and Internal Memorandums
5. Emails and other electronic communications
6. Legal files and Papers
7. Payroll documents
8. Pension documents
9. Personnel records
10. Tax records

In any case, all personal data will be retained for a minimum period which allows the Group to file a claim or defend itself in court under the local legislation.

4.6. Training of personnel

The Group ensures that all employees that have access to Personal Data will have their responsibilities under this Policy outlined to them as part of their staff introduction training. In addition, each member of the Group will provide regular Data Protection training and procedural guidance for their employees.

The Local Data Protection Officer is responsible for delivering the appropriate trainings to all Employees. The format of such trainings may vary depending on the target audience, number of employees to be trained, objectives of the training and other circumstances.

Trainings should be performed on regular basis. Each member of the Group establishes the concrete timeline on its own hence it should be in accordance with requirements/proposals of the Global or EU Data Protection Officer.

4.7. Records of processing activities

Each Group Company has mapped out all the Personal Data that it processes and controls and maintain it in a Data register (Annex 4).

This Data register ensures that the Group Companies complies with some of the main accountability requirements required under the GDPR:

- Maintaining records of all processing activities;
- Maintaining records of the data Processor agreements;
- Maintaining records of the data breaches, including breach notifications to supervisory authorities and Data subjects.

While the content of the Data register might vary between members of the Group, it contains at least the following records of the processing activities:

- the name and contact details of the Group and, where applicable, the (joint) Controller, and its representative;
- the purposes of the processing activities;
- a description of the categories of Data subjects and of the categories of personal data;
- the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations;
- where applicable, transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organizational security measures taken by the Group.

Each members of the Group is solely responsible for maintaining the register.

4.8. Data transfers

In order to compensate for a possible lack of Data Protection, transfers of Personal Data to counterparties, is subject to additional security measures. The Group has identified three different sets of data transfers within its organization, all with different sets of security measures:

- The intragroup data transfers: in order to facilitate transferring data Binding Corporate Rules will be implemented. These are rules approved by the supervisory authority which are legally binding on all members of the Group. Among other things these Binding Corporate Rules specify the purposes of the transfer and affected categories of data; reflect the requirements of the GDPR; confirm that the EU-based data exporters accept liability on behalf of the entire group; explain complaint procedures; and provide mechanisms for ensuring compliance (e.g., audits).
- Data transfers to counterparties within the EEA (or one of the other countries considered to guarantee the same protection) who act as Processor: these are data transfers under the GDPR.

  Prior to transferring any data to a third party, each member of the Group has made enquiries through due diligence processes and has assessed whether this counterparty complies with the applicable regulations.

  Following this assessment, each member of the Group has to conclude a contract with each of these third party Processors (a third party Processor's agreement). All of these agreements contain at least the following information:

- for the data transfers to non-Group entities outside the EEA and insofar as the GDPR applies (meaning: a member of the Group is located within the EU or the Data subject resides in the EU):

  In addition to concluding the abovementioned data Processor's agreement, each member of the Group shall check whether the counterparty to whom the Personal Data to be sent maintains an adequate additional safeguards. If such safeguards have not been taken, than the Group does not transfer any information to this third party.

4.9. Data Protection impact assessment

To ensure that all Data Protection requirements are automatically identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each member of the Group must ensure that a Data Protection Impact Assessment (DPIA) is conducted for all new and/or revised systems or processes for which it has responsibility.

This DPIA is conducted in cooperation with the Global and EU Data Protection Officer. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology uses on the security of personal data.

4.10. Data Protection Officers

4.10.1. The Data Protection Officers

Since the Group operates in different jurisdictions, including the EU, multiple Data Protection Officers are appointed:

- The Global Data Protection Officer (responsible for the Group):

  The Global Data Protection Officer is appointed and removed from the position by the CEO, upon having consulted with the General Counsel and the CFO.

  The Global Data Protection Officer of the Group is Aleksander Pusanov. His contact details are: Aleksander.Puzanov@eurochem.ru.

  The EU Data Protection Officer (responsible for the EU activities of the Group):

  The EU Data Protection Officer is appointed and removed from the position by the CEO, upon having consulted the Global Data Protection Officer.

  The EU Data Protection Officer of the Group is Pieter Callens. His contact details are: Pieter.Callens@eurochem.be

  The Local Data Protection Officers (responsible for a member of the Group if appointed):

Each member of the Group may appoint a Local Data Protection Officer. The Local Data Protection Officer is appointed and removed from the position by the CEO/general manager of the member of the Group. In case no Local Data Protection Officer has been appointed, the CEO/general manager will function as Local Data Protection Officer.

4.10.2. The responsibilities of the Data Protection Officers

Global Data Protection Officer

The Global Data Protection Officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of Data Protection law and practices and the ability to fulfil the following duties of Global Data Protection Officer:

- to advise the management of the Group on the Policy's matters and support them with major Data Protection risks, concerns and issues as they arise;
- to establish and ensure a high quality Data Protection System within the Group;
- to manage communications, educational or training strategies and initiatives and ensure support to the Business Units in the areas of Data Protection as required;
- to supervise the EU Data Protection Officer and Local Data Protection Officers (if appointed) .

In cooperation with EU Data Protection Officer and Local Data Protection Officers (if appointed):

- to ensure that appropriate procedures and policies are in place in the Group to keep Personal Data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors;
- to conduct regular trainings of Data Protection, to give explanations on the related matters and issues;
- to inform and advise the Group and the employees who carry out processing of their obligations pursuant to this Policy;
- to monitor compliance with this Policy and conduct audits;
- to provide advice where requested as regards the Data Protection impact assessment and monitor its performance;
- to monitor and analyze changes into applicable legislation;
- to review the retention dates of all the Personal Data processed by the Group and will identify any data that is no longer required in the context of the registered purpose;
- to make an appropriate arrangements where a counterparty may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the Personal Data to the counterparty where this is required;
- to consider the extent of possible damage or loss that might be caused to individuals (e.g. employees or counterparty) if a security breach occurs, the effect of any security breach on the Group itself, and any likely reputational damage including the possible loss of customer trust.

EU Data Protection Officer

The EU Data Protection Officer shall be a EU resident and shall be designated on the basis of professional qualities and, in particular, expert knowledge of Data Protection law and practices and the ability to fulfil the following duties in addition to the duties listed above:

- to cooperate with the EU supervisory authorities, the Global Data Protection Officer and Local Data Protection Officers (if appointed);
- to act as the contact point for the supervisory authorities on issues relating to processing and data breaches;
- to monitor and analyze changes into EU legislation and to report to Global Data Protection Officers on those changes.

Local Data Protection Officer

Each member of the Group may appoint the Local Data Protection Officer to assist the Global and EU Data Protection Officers in fulfilling of their abovementioned duties.

5. Policy Governance

5.1. Responsibility

Each member of the Group is solely responsible for compliance with this Policy, its legal obligations and appropriate processing of the personal data. Complying with the Policy requirements is mandatory for the employees involved in the processes.

If there is reason to believe that legal obligations contradict the duties under this Data Protection Policy, the member of the Group must inform the Global Data Protection Officer. In the event of conflicts between national legislation and the Policy, the Group will work with the relevant member of the Group to find a practical solution that meets the purpose of the Data Protection Policy.

If opportune, a member of the Group can adopt regulations that either complete or deviate from this Policy. These regulations need to be approved by the Global Data Protection Officer of the Group.

5.2. Controls

Each member of the Group guarantees that complying with the Policy requirements or alert about any breaches which might already happen or may potentially happen will not lead to any negative consequences for the subject employee. Meanwhile the Group will not accept any actions of employees which break the Policy.

The Group presumes and expects that employees will report any cases of the breach or potential breach of the Policy via the “Whistleblowing line”. Details of the line are publicly-available and are posted on the corporate portal.

The Group reserves the right to periodically check the employees’ knowledge on Personal Data Protection, to audit the performance and execution of this Policy and to make an analysis of its effectiveness.

5.3. Confidentiality

As described in article 4.4, Personal Data is subject to confidentiality obligations.

However, in certain circumstances, it is permitted that personal data is shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the Personal data is necessary for any of the following purposes:

• The prevention or detection of crime.

• The apprehension or prosecution of offenders.

• The assessment or collection of a tax or duty.

• By the order of a court or by any rule of law.

If any member of the Group processes personal data for one of these purposes, then it may apply an exception to its confidentiality obligation but only to the extent that not doing so would be likely to prejudice the case in question.

If any member of the Group receives a request from a court or any regulatory or law enforcement authority for information relating to a data subject, the entity must immediately notify the Global Data Protection Officer who will provide comprehensive guidance and assistance.

5.4. Policy review

This Policy shall be reviewed by the Global Data Protection Officer on a regular basis, but at least annually in order to ensure that the Policy is up to date and is in line with all applicable rules and legislation.

Any amendment will be reported immediately to the Group who will implement the amendments.

The latest version of the Data Protection Policy can be accessed at the Group website: www. eurochemgroup.com

5.5. Complaints and questions

All enquiries about this Policy and its annexes can be sent to the Global Data Protection Officer or the relevant Local Data Protection Officer.

Data Subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Global Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Global Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data subject and the Global Data Protection Officer, then the Data subject may, at its option, seek redress through mediation, binding arbitration, litigation, or via complaint to the relevant Data Protection authority within the applicable jurisdiction.

.

Annex 1. References

	ID	Document title	Remark
Regulatory document			
1		Compliance Policy EuroChem Group AG	
2		Code of Conduct EuroChem Group AG	
3		Federal Act on Data Protection (FADP)	

Annex 2. Data breach register

№	Member of the Group	Category of personal data	Description	№ of Data subjects affected	Contact details of Data subjects	Potential consequences	Measures taken/to be taken

Annex 3. Retention Schedule

№	Member of the Group	Category of personal data	Record type	Retention period

Annex 4. Data Register

№	Member of the Froup*	Category and description of personal data*	Purpose of the processing*	Categories of recipients*	Transfer to a third party	Time limits for erasure	Security measures

Columns marked with * are mandatory fields.