PAREX
Building expertise, together

SF39/1
Issue 1 Rev 1
Apr 2018

Protection of personal data

Protection of personal data Policy

Description of the document

Parex Ltd's Personal Data Protection Policy defines the risk coverage strategy for personal data.	Date	24/11/2017
	Version	1
	Status	Validated
	Writer	CONFIDENTIAL
	Validated by	CONFIDENTIAL

Modification authorisation

Data Protection Officers (DPO) & Personal Data Referents (DPO Referents)	Document changeable by the DPO and DPO referents Final document to be validated by the DPO and DPO referents

Broadcast list

Name	Department	Date
All employees	PAREX LTD	

History of the document			
Version	**Date**	**Modification**	**Writer**
1	24/11/2017	Initial version	CONFIDENTIAL
2	29/11/2017	Enhancements	CONFIDENTIAL
3	03/01/2018	Modifications	CONFIDENTIAL
4	04/04/2018	Modifications	CONFIDENTIAL

Table of Contents

Introduction

Parex Ltd's compliance with the rules on the protection of personal data is a factor of transparency and trust for its employees, former employees, customers, partners and rights holders.

This **Protection of personal data Policy** describes the strategic elements allowing PAREX LTD to ensure the protection of personal data collected in the course of its activities in accordance with the laws and regulations applicable in Europe.

The General Data Protection Regulation (GDPR) which comes into force on May 25, 2018 sets a framework for the collection and processing of personal data to strengthen the rights and freedoms of individuals.

This Policy applies to all persons and systems **handling personal data** within all PAREX LTD services and to its subcontractors.

The main risks related to personal data include:

- **The illegitimate access** to personal data
- **Unwanted modification** of personal data
- **The loss** of personal data
- **Failure to comply with the requirements** regarding the processing of such data as required by law and regulations
- **The impact on the image of PAREX LTD** in case of non-compliance with the regulations in force
- **Financial penalties in the event of a fine**, which can go up to 20 million euros or 4% of the global turnover to which can be added the costs related to the lawsuits of the victims.

This policy addresses the following issues:

- The **principles** relating to the processing of personal data
- **Roles and responsibilities** of data protection actors
- **The rights of data subjects** to the processing of their personal data.

1. Collection of personal data

<u>What is personal data?</u>

Any information relating to an identified or identifiable physical person (referred to as "the data subject")

*Identifiable physical person = a physical person **who can be identified**, directly or indirectly, in particular by reference to an identifier, such as a **name**, an **identification number**, **location data**, **online identifier**, or one or more specific elements specific to its **physical**, **physiological**, **genetic**, **psychological**, **economic**, **cultural** or **social***

Directly personal: Name, Surname, Image, video, biometric data (thumbprint, image of the retina ...)

Indirectly personal: customer number, National Insurance number, employee number, IP address, Bank details, GPS tracking

What is sensitive data?

Sensitive data is any data that reveals:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health or a natural person's sex life and/or sexual orientation

What is processing?

It is any transaction or set of transactions that may or may not be performed using automated processes and applied to data or sets of personal data.
Types of processing = collection, recording, organisation, structuring, preservation, adaptation or modification, extraction, consultation, use, transmission, dissemination, reconciliation or interconnection, limitation, erasure or destruction.

Main obligations of the Parex Ltd Employee

1 -I IDENTIFY THE PERSONAL DATA THAT I COLLECT

For example Personal data of employees or potential employees?

For example Personal data of a legal person contact (Customer, Supplier, Provider ...)?

For example Personal data of a Prospective customer supplier or provider?

2 - I DEFINE THE PURPOSES OF MY PROCESS

For example Employee integration process in the company via a tool

For example Creating a client file using a tool

For example Sending emailing to prospects for business purposes

3 - I AGREE TO FOLLOW THE FOLLOWING REQUIREMENTS

1 **Inform**
- The person whose personal data have been collected of his rights and obtain his prior consent when my process so requires;

2 **Ask the LDC (Local Data Correspondent)** before any negotiations with a new Service Provider to ensure compliance with the PAREX LTD internal policy for the protection of personal data (e.g. drafting contractual clauses for a new contract or an amendment)

3 **Perform the authorisation formalities** to the Supervisory Authority with the support of the LDC when my process requires it

4 **Conduct a privacy impact assessment** with the support of the IT Dept and LDC when my process requires it

I am GDPR compliant

2. Organisation

2.1. Roles and responsibilities

Data protection is the responsibility of everyone and in particular, it applies:

- To employees who must respect this policy
- To directors who are responsible for ensuring that their processing complies with this Policy and that it is respected by their teams
- To the LDC (Local Data Correspondent) who puts in place the appropriate procedures, protective measures and controls
- To the DPO (Dapta protection Officer) has overall responsibility for GDPR within ParexGroup
- To the internal audit which provides an independent guarantee of compliance

These stakeholders are technically assisted by experts from the functional departments: IT Department, legal, purchasing, IT Security...

Employees

Employees comply with the provisions of the Policy and in particular do not bypass the security features in place.

They also pay particular attention to messages or awareness-raising sessions related to the protection of personal data.

They use the personal data in accordance with the registered processes and inform their manager and the Local Data Correspondent of any **possible data security breach**.

Data Protection Officer, DPO, Parex Group

The DPO ensures the **first level of protection of personal data** after the employees. As such:

- They associate the regulatory requirements with those of PAREX LTD. In accordance with these requirements, they ensure their compliance throughout the lifecycle of the personal data used.
- They ensure that their teams comply with the data protection rules and send any information to the local data correspondent that is necessary for them to carry out their action.
- They provide adequate communication to their teams and sensitise them to the protection of personal data with the help of the local data correspondent
- They have regular exchanges with the Local Data Correspondent and keep him informed of any changes (organisational or other) that may impact data protection.

The directors of the functional departments, if necessary, make their experts available to the DPO.

Local Data Correspondent (LDC)

The LDC is the **expert and guardian of the protection of personal data**. He must be associated with any questions relating to the protection of personal data.

Each Data Controller must therefore check with the LDC that the processing for which he / she is responsible has been the subject of the required preliminary formalities.

The LDC is the second level of data protection with varied missions:

- Set up the "Personal Data" infrastructure dedicated to the implementation and maintenance of compliance of Personal data: documents (policies, procedures, ...), governance / processes (incident reporting ..), small tools (register of process, grid of risk analysis ...), Organisation of training ... especially in project and contracting phases
- Ensure a regulatory watch
- Being the expert, providing advice to all stakeholders (Parex Ltd, subcontractors)
- Liaise with the Supervisory Authority – the Information Commissioner's Office, ICO (request for information, control, incident)
- Coordinate and manage responses to incidents involving personal data (unauthorised access, data breach, etc.)
- Assist in the preparation of internal or external confidentiality agreements (subcontracting with possible transfer outside the European Union)
- Update the "Personal Data" repository: Processing register, policies and procedures, security analyses and action plans...
- Raise awareness and train the various stakeholders.

The expectations of a local data correspondent are those of a DPO, except the transversal task of monitoring subsidiaries which is the role of the DPO.

Internal audit

Internal audit provides **the third level of data protection.**

It verifies that personal data protection requirements are taken into account during its business audits within Parex Ltd.

It ensures the effectiveness of the measures put in place to protect the data.

3. Principles

3.1. Regarding the data

Transparency principle

Data must be treated fairly, lawfully and transparently.

Individuals must be informed in advance of any collection and use of their personal data (via collection forms, contractual documents, company policies, etc.). This information must be complete and easy to understand.

Practical cases:

- **In the contracts**
- **In the clauses**

Limitation purpose principle

Personal data are collected for specified, explicit and legitimate purposes and are not further processed in a manner incompatible with those purposes.

Therefore, collected data cannot be used for processes not originally specified to the data subject.

Examples of purposes: Recruitment management, Training management, Savings plan management

For example, a CV cannot be used for commercial offers

Principle of data minimisation

The processed data must be relevant, adequate and limited to what is necessary for the purposes for which they are processed.

It is thus possible, for the sending of commercial information to prospects to collect emails, but in no way to collect bank details or to ask for the National Insurance number.

Principle of data accuracy

The processed data must be accurate and regularly updated (rectification or deletion).

Parex Ltd takes all reasonable measures to ensure that inaccurate data are promptly rectified or deleted (taking into account reports, setting up regular reviews of data).

For example, taking into account the modification of personal data sent by a customer (update on Winman)

Principle of data retention limitation

PAREX LTD retains personal data as long as the purpose or the regulations require. Beyond that, the data is deleted or anonymised.

The retention period of the data should **be kept to a minimum.**

Integrity and data confidentiality principle

The data must be processed in such a way as to ensure appropriate security of the data.

Technical or organisational measures must be put in place to ensure appropriate data security and thus avoid loss / destruction / accidental modification or breach of information.
An Excel list containing personal data can be protected by a password.

3.2. Regarding processing

A process can only be implemented if it is lawful (principle of lawfulness).

To this end, it must comply in advance of its implementation to one of the following conditions:

Consent	the person concerned has consented to the processing of his / her personal data for one or more specific purposes
Contract	the processing is necessary for the performance of a contract with which the person concerned is involved or for the performance of pre-contractual measures taken at the request of that person
Legal obligation	the processing **is necessary to comply with a legal obligation** to which the controller is subject
Legitimate interest	the processing is necessary for the **legitimate interests** pursued by the controller or by a third party, unless the interests or fundamental rights and freedoms of the person concerned which require the protection of personal data prevail

By default the processing of personal data is prohibited, which reveal:

- racial or ethnic origin, data concerning sex life or sexual orientation
- political opinions, religious or philosophical beliefs
- trade union membership
- biometric data for uniquely identifying a physical person
- data concerning the health of a physical person

These processes may nevertheless be authorised if the person has given his explicit consent and if a Privacy Impact Assessment (PIA) has been carried out and validated. This could be requested by the control authority (ICO) in case of control.

Authorisation requests

Under the current Data Protection Act (DPA), organisations that process personal information are required to notify with the ICO as Data Controllers. They are also required to pay the ICO a notification fee, based on their size. When the GDPR comes into effect there will no longer be a requirement to notify the ICO in the same way. The new model will start on April 1st 2018.

Subcontracting

Parex Ltd only uses subcontractors who provide sufficient guarantees for the implementation of technical and organisational measures.

This implementation and control are the responsibility of:

- The Local Data Correspondent with the help of internal experts (Data Controllers...) during the contractualisation phase and renewal of the contract
- The Data Controller during the execution of the contract.

Data transfer abroad

A transfer of personal data to a third country outside the European Union **cannot be done without the prior approval of the Local Data Correspondent.**

4. Data subjects rights

Physical persons (employees, partners, customers and prospects) have rights and may request in writing to exercise them at any time.

Right to be informed

PAREX LTD informs the data subject, at the time of the data collection and for each process, of the following points:

- The identity and contact details of the data controller
- The contact details of the local data correspondent
- The purposes of the processes
- The recipients or the categories of recipients of personal data
- The retention period of the data
- If applicable, the fact that the data will be transferred to a third country and the fact that Parex Ltd has been authorised for this process
- The rights of the data subject (access, rectification, deletion, processing limitation, processing opposition, portability, complaint to a Supervisory Authority)
- The existence of a possible automated decision-making based on these data
- The means to contact PAREX LTD in order to assert its rights, including an electronic means of contact if the collection is done electronically.

This information should be given:

- if the collection is direct: at the time of data collection
- if the collection is indirect: During the first communication with the data subject and not more than one month after obtaining the data.

The information must be **concise, transparent and understandable.**

Right of access and rectification

The data subject has a right of access to the data and a right of rectification.

Any physical person justifying his identity may exercise his right of access to data concerning him by a simple written request to the Local Data Correspondent (who will contact the Data Controller).

The data subject has the right to obtain a correction of the personal data concerning him as soon as possible from the Data Controller.

Parex Ltd shall notify each recipient to whom the personal data have been communicated for any rectification, unless such communication proves impossible or requires disproportionate effort.

Right to limit a process

Parex Ltd limits the processing of personal data of any person who requests it in writing, subject to compatibility with the regulatory obligations of PAREX LTD. PAREX LTD can no longer process the data (except for archiving if applicable).

The purpose limitation can only apply in the following cases:

- The accuracy of the personal data is disputed by the data subject. Parex Ltd should verify the accuracy of the personal data
- The process is unlawful and the data subject opposes the deletion of its personal data and instead requires the limitation of their use
- Parex Ltd no longer needs personal data with regard to the purpose of the process, but it is still necessary for the data subject to exercise or defend his legal rights
- The data subject objected to the process. Parex Ltd should check whether the legitimate grounds pursued by PAREX LTD override those of the data subject).

Parex Ltd informs the data subject before any lifting of limitation.

Right to object to a process

The right to object, on the other hand, is unconditional if the data are used for prospecting purposes. In other cases, the reasons and interests of the data subject and those of the Data Controller should be balanced.

For example, the data subject cannot oppose a process if it is necessary for:

- the performance of a contract to which the data subject is a party
- The compliance of a legal obligation to which the Data Controller is subject.

Right to be forgotten

A right to deletion (or right to be forgotten) applies when the data are no longer needed, when the person withdraws his consent, when his right to object applies, and when the process is unlawful or when the law obliges to delete the data. This right does not apply in case of a legal obligation.

If he has published the data, the Data Controller must also make the request for deletion known by reasonable measures to those who have been able to reuse it.

Parex Ltd transmits the instruction to the set of co- Data Controllers or subcontractors concerned to delete the data.
Parex Ltd retains and applies guidelines for the fate of its personal data after death, to any appropriate person who requests it.

Right to portability

Parex Ltd sends, in a structured format, commonly used and machine readable, the personal data of any person who has made the request in writing, always subject to compatibility with regulatory obligations.

This portability can only take place if the data has been provided by the person and if the two following conditions are met:

- The process is based on consent or on a contract
- The process is performed using automated methods.

Parex Ltd transmits directly to another Data Controller the personal data of any appropriate person who has made a request in writing, when it is technically possible

Response time

The response to any request in writing must be made within one month after receiving the request.
The answer must be concise, understandable and must not infringe the rights of others.
No payment may be required by PAREX LTD, unless clearly excessive, e.g. in the case of repetitive requests.

5. Appendices

5.1. General requirements

Accountability

The principle of "accountability" refers to the obligation for companies to implement internal mechanisms and procedures to demonstrate compliance with the rules on the protection of personal data. Especially:

- The adoption of internal rules
- The obligation to keep track of decisions and process carried out
- Conducting a Privacy Impact Assessment for processes that have a special risk with regard to the rights and freedoms of data subjects
- The adoption of the "Privacy by Design" and “Privacy by Default” approaches (definition below)
- The appointment of a Local Data Correspondent (LDC) who controls Personal Data compliance within a Parex Ltd perimeter
- The establishment of continuous monitoring.

Companies must act and be able to trace and prove what has been done.

Data security

Organisational and technical security measures must be implemented to ensure the integrity and confidentiality of personal data. The purpose of these measures is to prevent destruction, loss, alteration and unauthorised disclosure.

The following measures should therefore be provided:

- authorisation and authentication management
- awareness and training
- traceability and logging of accesses and actions on the data
- security of equipment (PC, smartphone, tablet ...) and the network, including encryption
- business continuity
- incident management
- physical security
- anonymisation and pseudonymisation of data
- monitor network and system activity.

It should be noted that securing also concerns non-computerised processes and tools.

Privacy by Design

The Integrated Privacy Protection (Privacy by Design) is a concept that means taking into account personal data protection requirements **when designing a new project or product**.

Privacy by Default

The Privacy by Default applies in the continuity of the Privacy by Design. The company must take care to limit the amount of personal data processed when designing a new project or product and use only the personal data deemed necessary.

Training / awareness

Parex Ltd employees must be made aware of and trained in good practices related to the protection of personal data. **Providers must be trained by their employers**.

Incident response

Any violation of personal data (at Parex Ltd or one of its subcontractors) must be communicated to the LDC for notification to the supervisory authority no later than 72 hours after Parex Ltd or the subcontractor has acknowledged it.

The data subject must also be informed if the breach is likely to cause high risks.
Note: The Incident Management Procedure is specified in SF39/2 Personal Data Breach Management"

Impact analysis on data protection

When a type of processing is likely to create a high risk for the rights and freedoms of physical persons, Parex Ltd shall carry out, before processing, **an analysis of the impact of the processing operations envisaged on the data subject's personal data**.

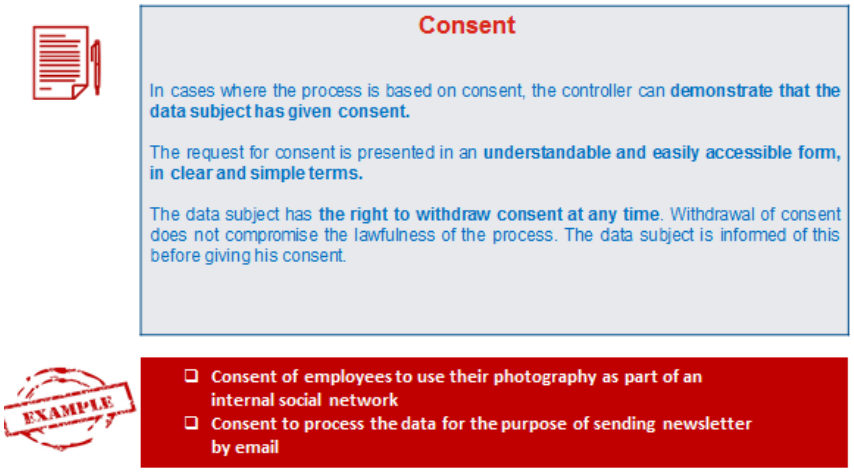
The Data Controller validates the impact assessment completed by the LDC.

Note: The impact analysis for data protection is also described in the document: "Privacy Impact Assessment Procedure (PIA)".

5.2. Lawfulness of processing

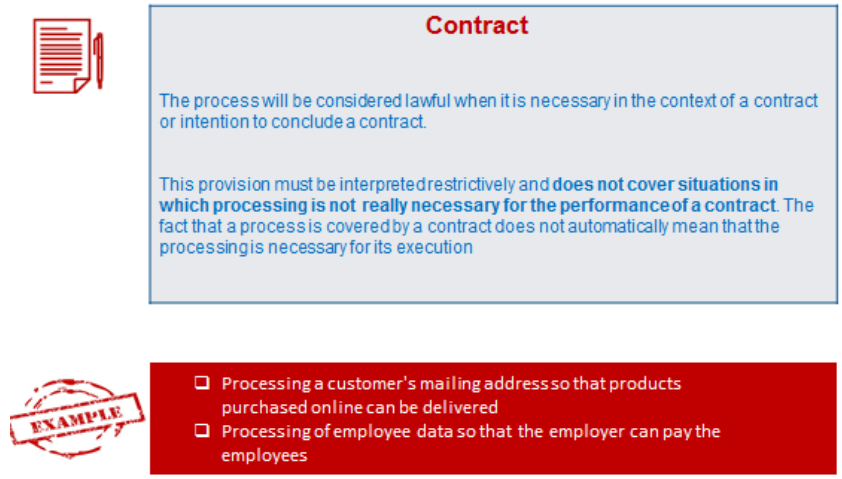
Consent

Parex Ltd is able to show that the data subject has given his consent to the processing of his personal data.



Contract

The processing is necessary for the performance of a contract to which the data subject is a party.



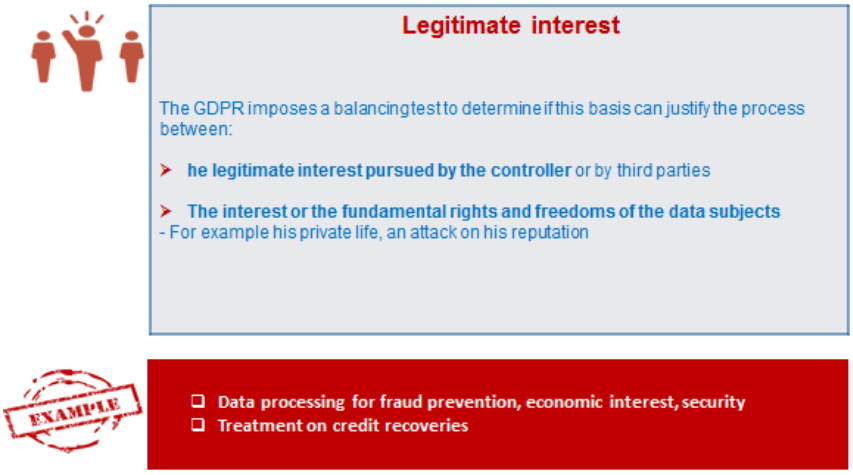
Legal obligation

The process is necessary to fulfill a legal obligation.

Legitimate interest

The processing is then deemed necessary by Parex Ltd for the execution of its services.

This reason "Legitimate interest of Parex Ltd" is evaluated by Parex Ltd on the basis of the balance of an interests test:
"Does the legitimate interest of the controller override the interest of the data subject?"



5.3. ICO Articles

a. https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/
b. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
c. https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

** End of the document **