Principles of processing and protection of personal data

Each company of the PFNonwovens group of companies; including in particular PFNonwovens US Inc. and PFNonwovens LLC with the registered office in the USA, PFNonwovens Holding s.r.o, PFNonwovens a.s., PFN International Services s.r.o., PFNonwovens Czech s.r.o., PFN – NW a.s., PFN – NS a.s. and PFN - GIC a.s. with the registered office in the Czech Republic, PFNonwovens Egypt LLC with the registered office in Egypt and PFNonwovens RSA (PTY) LTD with the registered office in the Republic of South Africa (the "PFN Group" or "the Group") is committed to protecting the privacy and security of data subject's personal data.

These Principles of Processing and Protection of Personal Data (hereinafter also referred to as simply our "Privacy Policy") provide information about which personal data of individuals (also referred to as "data subjects") are processed within the Group (also referred to as "Us"/"We"), and fulfil the information obligation of the companies of the Group according to the relevant legal regulations, in particular Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46 / EC (General Regulation on the protection of personal data) (hereinafter also referred to as the "GDPR Regulation").

A more detailed structure of the Group can be found here.

PFN Group companies with the registered offices in the Czech Republic are joint controllers of personal data and agreed that PFNonwovens Holding s.r.o., with its registered office Hradčanské náměstí 67/8, Hradčany, 118 00 Prague 1, Czech Republic, ID No.: 04607341, will act in respect of the data subjects as the central point of contact and will fulfil the duties arising from the applicable legal regulations, in particular, the GDPR, for the benefit of data subjects.

This Privacy Policy describes how we collect and use personal data, in accordance with the applicable data protection laws across the jurisdictions in which PFN operates, including the European General Data Protection Regulation ("GDPR"). It applies to applicants to job offers proposed by PFN. We may update this notice at any time in accordance with the procedure described below.

A) On whom do we process personal data?
In the scope of our act activities, we process personal data on the following categories of data subjects:

- Job applicants
- Employees or members of statutory or other elected / appointed bodies
- Business partners, such as customers, suppliers, etc.
- Other third parties, such as people entering a Group facility, visitors to our website, etc.

In the event of processing the personal data of other categories of data subjects, the provisions of this Privacy Policy that are closest to the personal data processed will be used for the fulfilment of information obligation.

B) What personal data do we process? How is personal data collected?
We may collect personal data using various ways, including, but not limited to:

- disclosed directly by data subjects, whether orally or in writing;
- received by third parties which may lawfully administer information on data subjects;
- accessible from publicly available information (e. g. public registers).

Specifics regarding the personal information of Group employees, are addressed separately by the internal work procedures / directives of the Group.

Job Applicants
For job applicants, the information how we collect and use their personal data is described in separate PFNonwovens Applicants Privacy Policy (available here).

Business Partners
In the case of our business partners, whether they are sellers, buyers, service providers, gifted, contractors, customers, etc., we process such personal address and identification information as our business partners provide us with; potentially personal data originating from publicly available registers, such as the Commercial Register, the Trades Licensing Register, the Insolvency Register, the Cadastre of Real Estate, etc., in particular:

- Name and last name
- Permanent residence, mailing address

- Date of birth, possibly ID number
- Work e-mail address
- Work phone number
- Bank account
- Job title
- ID, Taxpayer ID
- Signature

Other Third Parties
For other third parties, such during e-mail or document communication, visiting our production facilities, visiting websites, etc., we process personal address and identification information provided by the third parties themselves, or potentially, are available from camera records, especially:

- Name and last name
- Work e-mail address and work phone number
- Job title
- Signature
- Image and visual information on behavior and actions of recorded persons (for video camera recordings)
- IP address (for website visitors)

As for using cookies on our website, you can find more information in our Cookies Policy (available here).

C) For what purpose, on what legal basis, and for what duration do we process/store personal data?

Job Applicants
For job applicants, the information how we collect and use their personal data is described in separate PFNonwovens Applicants Privacy Policy (available here).

Business Partners
We process the personal data of business partners for identification of the contracting parties, mutual communication, performance of the contract, verification of the ability to meet obligations and further, for potential future application and protection of the rights and obligations of the contracting parties.

Such processing of personal data is necessary for the performance of the contract, fulfilment of legal obligations and also for the purposes of our legitimate interests, without requiring consent to the processing of personal data. We process this personal data for the period of our mutual cooperation and further for a period of 10 years from its termination, and potentially for an additionally necessary period.

Other Third Parties
Within the context of electronic or document communications, visits to our production facilities, or when visiting our website (separate from camera recordings and IP addresses – see below), the personal data of other third parties is processed for identification of the contracting parties, communication, familiarization with instructions, OSH obligations and rules of conduct in our premises and for the future, eventual application and defence of the rights and obligations of the parties.

Such processing of personal data is necessary for the performance of the contract, fulfilment of legal obligations and also for the purposes of our legitimate interests, without requiring consent to the processing of personal data. We process this personal data for the period of our communication (or facility visit) and further for a period of 10 years from its termination, and potentially for an additionally necessary period.

Camera Recordings
We process the personal data captured on the basis of video camera recordings (especially likeness and visual information on the behaviour and actions of recorded persons; audio recordings are not captured, stored or processed in any way by camera systems) to protect the assets of Group companies and protect the property of our employees and others against theft and vandalism, as well as prevention of theft and vandalism, protection of the health of the end users of our products, protection of work safety and controlling of the technological and manufacturing process.

Such processing of personal data is necessary for the purposes of our legitimate interests, without requiring the consent of third parties to the processing of personal data.

Due to non-stop operation of our manufacturing facilities, our production lines are continuously monitored by camera equipment, 24 hours per day / 7 days per week. Other cameras with motion sensors record only in the case of detection of motion.

Places that are monitored by camera systems with recording, are marked for the duration of operation of the camera systems with the appropriate, clearly visible sign bearing the relevant pictogram / image of a camera, and the words "CCTV monitored and recorded".

Records from cameras are stored in time loops, i.e. after the specified recording retention time, the recording loops are automatically overwritten. The retention time depends on the amount of disk space, the number of scanning cameras, and the purpose of processing. If an incident is detected, the record is retained for the period of time necessary for discussion before bodies involved in criminal proceedings, or potentially, other interested entities for the fulfilment of the purpose of the processing.

IP addresses
We process IP addresses to ensure network security.
Such processing of personal data is necessary for the purposes of our legitimate interests, without requiring consent to the processing of personal data.
We process this personal data for a period of 2 years, or potentially for another, necessary period of time.

D) Who may have access to personal data? Where will we transfer data subject's personal data?

Access to personal data, if necessary for the fulfilment of the purpose of processing, in particular for the performance of a contract or legal obligation, may be granted to all companies in the Group and limited number of authorized employees of the PFN Group.

We may transfer personal data within the PFN Group, including outside the European Union (EU) and European Economic Area (EEA). Where we transfer personal data outside of the EU or EEA, we will implement appropriate and suitable safeguards to ensure that such personal data will be protected as required by applicable data protection law.

Where personal data is transferred within PFN Group, the safeguards which we typically put in place are data transfer agreements compliant with the European Standard Contractual Clauses.

We may disclose personal data to third-party providers, agents or contractors that provide us services which require the processing of personal data, and only for purposes provided in this Privacy Policy. We will only personal data to any third-party provider, agent or contractor that provide assurances that it will protect personal data disclosed to it in accordance with the provisions of this Privacy Policy and pursuant to a written agreement binding over such provider, agent or contractor.

Where personal data is transferred to any third party, and where it is mandated by applicable law, we implement the appropriate measures to ensure that personal data is treated by the recipients in a way that is consistent with and which respects the applicable privacy and data protection laws through the execution of standard contractual clauses or any other relevant mechanism recognized by the GDPR.

For further information as to the safeguards we implement please contact our Privacy team by e-mail at the addresses indicated in Article G – Contact.

Categories of third parties that may have access to personal data:

- The persons who provide us with the technical operation of the website (e.g. access to IP addresses of website visitors),
- Persons involved in the operation of camera systems (e.g. for camera recordings),
- Persons providing security services of production areas (e.g. personal data of facility visitors),
- Persons managing information systems (e.g. personal data of customers),
- Other persons, if necessary to fulfil a contract or other obligations (e.g. personal data of customers to carriers or other parties involved in the performance of the contract).

Based on applicable legislation and subject to certain conditions, we are required to transfer some of data subject personal data to, for example, law enforcement authorities (for example, in the case of commission of a crime /

offense) or other interested parties (insurance companies, banks, and financial authorities and other public administration authorities).

All employees of the Group involved in the processing of personal data are under an obligation of confidentiality and treat personal data as confidential information. Also, other recipients of personal data (e.g., processors) are contractually bound by the confidentiality obligation and may not use the data provided for any purpose other than that we have provided to them.

E) What rights does a data subject have in relation to the protection of personal data?
Every data subject has, in particular the following rights in relation to personal data:

- The right to access the subject's personal data (commonly known as a "data subject access request"). This enables data subject to receive a copy of the personal data we hold about him and to check that we are lawfully processing it.
- The right to correct or supplement personal data that we hold about data subject. This enables you to have any incomplete or inaccurate information we hold about data subject corrected.
- The right to delete personal data (the right to be "forgotten") in certain cases. This enables data subject to ask us to delete or remove personal data where there is no good reason for us continuing to process it. Data subject also has the right to ask us to delete or remove his personal data where data subject has exercised his right to object to processing.
- The right to request processing restrictions in certain circumstances. This enables data subject to ask us to suspend the processing of his personal data, for example (i) where data subject thinks his personal data is inaccurate and only for such period to enable us to verify the accuracy of his personal data; (ii) the use of his personal data is unlawful and data subject opposes the erasure of his personal data and requests that it is suspended instead; (iii) we no longer need his personal data, but his personal data is required by data subject for the establishment, exercise or defence of legal claims; or (iv) data subject has objected to the use of his personal data and we are verifying whether our grounds for the use of his personal data override his objection.
- The right to raise an objection or complaint against processing in certain cases, where we are relying on a legitimate interest (or those of a third party) and there is something about data subject's particular situation which makes data subject want to object to processing on this ground. Data subject also has the right to object where we are processing his personal data for direct marketing purposes.
- The right to request the transfer of data. This enables data subject to obtain his personal data actively and knowingly provided us with in a structured, commonly used and machine-readable format and for it to be transferred to another organisation, where it is technically feasible. The right only applies where the use of his personal data is based on data subject's consent or for the performance of a contract, and when the use of his personal data is carried out by automated (i.e. electronic) means.
- The right to withdraw consent at any time in the limited cases where data subject has provided his consent to the collection, processing and transfer of his personal data for a specific purpose. To withdraw a consent, you may contact our Privacy team at the addresses indicated below in Article G – Contact. Once we have received notification that data subject has withdrawn his consent, we will no longer process his information for the purpose or purposes he originally agreed to, unless we have another legitimate basis for doing so in law. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
- The right to be informed of breaches of personal data in specific cases.
- Other rights set out in the relevant legislation, namely in the GDPR Regulation.

Data subject can review, verify, correct or request erasure of his personal data by contacting our Privacy team at the addresses indicated below in Article G – Contact.

If, in the case of requests by data subjects applying the abovementioned rights, we have reasonable doubts as to the identity of the data subject who submits the application, we are unable to identify the data subject, we may request the data subject to provide the additional information necessary to confirm his / her identity and verification of identity.

Applications may be submitted by the data subjects in writing to the below address of the joint administrators. In the case of clearly unjustified or disproportionate requests (or in the case of provision of additional copies of personal data processed), a reasonable fee may be imposed on the data subject, taking into account the administrative costs involved.

F) Changes to Privacy Policy

We reserve the right to change and update this Privacy Policy at any time. We are then allowed to publish the amended versions on our website instead of the current version of the Privacy Policy, without any notice. It is the duty of data subjects and their responsibility to regularly monitor the wording of this Policy.

G) How can a data subject contact us?

If you have any questions about this Privacy Policy, please contact the Privacy team at : privacy@pfnonwovens.com; or to one of the following addresses :

- For the US: 101 Green Mountain Road Humboldt Industrial Park Hazleton, PA 18202, USA
- For Czech Republic: Hradčanské náměstí 67/8, Hradčany, 118 00 Prague 1, Czech Republic
- For Egypt: Plot No. O6,O8 in Zone No. 3 at the Northern Expansions Area and its Extension, 6th of October City, Giza, Egypt
- For RSA: 6 Charles Matthews Street, Atlantis Industrial, Cape Town, 7349, RSA

To keep records of the fulfilment of our obligations arising under applicable legislation, especially the GDPR Regulation, and the future application and protection of the rights and obligations of the parties, all communication between us and the data subject is monitored.

Data subject has the right to make a complaint at any time with his national data protection authority or other public authority governing the protection of his personal data. We would however appreciate the chance to deal with data subject's concerns before you approach such regulatory authority so please contact the Privacy team in the first instance.

The competent supervisory authority in the Czech Republic is the Office for the protection of personal data. Full details regarding the language requirements and the form of the complaint may be accessed on the website of the Office for the protection of personal data: https://www.uoou.cz/.

The competent supervisory authority in South Africa is the Information Regulator. Full details regarding the language requirements and the form of the complaint may be accessed on the website of the Information Regulator: https://www.justice.gov.za/inforeg/.

The competent supervisory authority in Egypt is the Personal Data Protection Center. Full details regarding the language requirements and the form of the complaint may be accessed on the website of the Information Regulator: https://www.justice.gov.za/inforeg/.

The competent supervisory authority in Pennsylvania is the Attorney General. Full details regarding the language requirements and the form of the complaint may be accessed on the website of the Information Regulator: https://www.attorneygeneral.gov/taking-action/press-releases/attorney-general-josh-shapiro-takes-action-to-preserve-pennsylvania-authority-to-protect-consumers-against-data-breaches/.