Global Data Protection Policy

of the Armacell Group | Version 1, September 2021

Contents

1. Introduction p. 2

2. Applicability p. 2

3. Principles for processing personal data p. 2

    3.1. Lawfulness p. 3

    3.2. Fairness and transparency p. 3

    3.3. Purpose limitation p. 4

    3.4. Data minimisation and storage limitation p. 4

    3.5. Accuracy p. 4

    3.6. Integrity and confidentiality p. 4

    3.7. Accountability p. 4

4. Transfers p. 4

5. Individuals' rights p. 5

    5.1. Right of access p. 5

    5.2. Right to rectification p. 5

    5.3. Right to erasure p. 5

    5.4. Right to data portability p. 5

    5.5. Right to object to direct marketing p. 5

6. Data protection impact assessment (DPIA) p. 5

7. Data protection by design and default p. 6

8. Data Protection Officer p. 6

9. Training p. 6

10. Amendments p. 6

11. Contact p. 6

Annexes

2 |Examples of personal data p. 7

3 |Information to be notified to individuals p. 8

For the sake of better readability, this policy uses only the male form. This is to be understood as also incorporating the female or any other form.

1. Introduction

The term “data protection” can refer to many things. The subject of this policy is handling the personal data individuals entrust us with carefully. This policy covers all employees, contractors, customers, vendors, potential applicants, and any other individuals where the collection of personal information may be required to do business.

Awareness for data protection has grown over recent decades. In some countries, the right to information self-determination is even a fundamental right comparable to human rights. As a result, data protection regulations have become much tighter globally over the last twenty years.

In a nutshell, data protection laws have two goals: Firstly, to provide for principles that must be observed when dealing with personal data. Secondly, to provide for rights of individuals to understand, and sometimes control, how their personal data is used, processed, stored, transferred, etc. In order to urge businesses to observe data protection laws more strictly, the maximum fines for non-compliance have been increased dramatically.

This policy will help to ensure that we comply with applicable data protection laws, thereby respecting the data protection rights of the individuals concerned and avoiding adverse consequences for our company. We are relying on you, the owners of the relevant data processing processes to implement this policy in our day-to-day business.

The Policy is not an exhaustive commentary of all global data protection laws. We have limited it to what is typically relevant at Armacell. Therefore, if something doesn’t seem to make sense for you, it might be worth checking with the Data Protection Officer to see if there is a different legal angle that this policy does not address.

Where the applicable data protection laws require a higher standard of protection for personal data than that set out in this Global Data Protection Policy, the requirements of the applicable data protection law shall prevail. Where the applicable data protection laws establish a lower standard of protection for personal data, the requirements of this Global Data Protection Policy shall prevail.

2. Applicability & definitions

The Global Data Protection Policy applies to the global organisation of Armacell entities for all dimensions and activities in all geographies where we operate.

The policy governs our processing of “personal data”. In this policy, “personal data” is any information that relates to an individual (i.e. a natural person) whose identity is either known or who can be identified. Annex 2 contains several examples of “personal data” and also examples of “special categories of personal data”, which require extra safeguards according to some local laws.

“Processing” within the meaning of this policy means doing anything with personal data, including collecting, storing, using, transferring, amending or even deleting it.

“Controller” means the natural or legal person, public authority, agency or other body that, alone or together with others, determines the purposes and means of processing personal data.

“Processor” means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

“Personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Principles for processing personal data

The following sets out the high-level principles that underlie Armacell's practices for collecting, using, disclosing, storing, securing, accessing, transferring, or otherwise processing personal data.

3.1. Lawfulness – Justification

Any processing of personal data requires that either:

(a) The processing is necessary for the performance of a contract (or for entering into a contract) between Armacell and the relevant individual,

"Necessary" means that we could not properly perform, or enter into, the contract without processing the data. Employment contracts are a typical example of a case where a contract justifies the processing of personal data. In order to perform the employment contracts with our employees, we need to collect, store, use, amend and sometimes transfer personal data such as their residential address or bank details.

(b) the individual in question has granted his consent to the processing,

Such consent must be given on an informed basis. This requires that we have informed the individual who we are, what personal data we intend to process, in which ways we intend to process it and for what purpose; who the recipients of his personal data are and where they are located and also of the fact that he has a right of revocation. Processing beyond the defined scope of the consent would require new consent (or another justification). When informing the individual according to the above, we point out that he can, in general, revoke his consent at any time. The consent must be fully documented, preferably in written or electronic form, as the burden of proof is on Armacell. The consent must be unambiguous and given freely.

Note that it will often be more suitable to integrate the consent into a document that is being signed by the relevant individual anyway. When combining the consent with another document, please note that it must be highlighted compared to the rest of the document.

(c) the processing is necessary for compliance with a legal obligation of Armacell or

For example, certain countries require that employers deduct and pay church tax as part of the monthly payroll process. In order to be able to comply with this legal obligation, employers in these countries need to know the religion/religious denomination of their employees.

(d) a legitimate interest of Armacell.

Personal data processing is lawful if it is necessary for the purpose of a legitimate interest of Armacell (or another person) unless such legitimate interest is outweighed by the rights or interests of the relevant individual. An interest in this sense could be any goal that Armacell is pursuing. Legitimacy requires that such a goal is legal. For example, part of the processing of the personal data of employees is typically based on legitimate interest (as it is not necessary for the performance of the employment contract). It is essential to weigh up carefully whether the legitimate interest we are pursuing is outweighed by the rights or interests of the individual. How important is our legitimate interest compared to the individual's rights or interests that are affected? And are there individual's rights or interests profoundly affected or merely superficially? Note that legitimate interest does not justify processing sensitive personal data (as defined in Annex 2).

3.2. Fairness and transparency – Notification

All processing of personal data must be fair and transparent. The individual must be provided with the information listed in Annex 3 ("Notification"). The notification must be made at the time when personal data is obtained (irrespective of whether the individual has requested the information or not). No notification is

required if the individual already has the information. For example, when we process personal data based on the individual's consent, we can include all the information required in the consent document.

3.3. Purpose limitation

Personal data is obtained and processed for one or more specific purposes. These purposes are fixed and documented, at the latest when we notify the individual. As soon as we intend to process the personal data for another purpose, we must confirm the lawfulness once more and prepare an amended notification.

3.4. Data minimisation, storage limitation

When we collect personal data, we must limit the collection to what is necessary for the purpose for which the personal data is collected. Likewise, we must limit the access to the personal data we have collected to staff that needs to have access. Similarly, personal data must be kept only for as long as it is necessary for the purpose for which we process it. Once we no longer need the personal data we must either delete or anonymise it (or, if it is subject to statutory archiving obligations, archive it in line with our document retention policies, further limiting access to the personal data).

3.5. Accuracy

We must take all reasonable steps to ensure that the personal data we hold is accurate and up to date in view of the purpose for which we process it. This includes rectifying or deleting inaccurate personal data or completing incomplete personal data.

3.6. Integrity and confidentiality

When processing personal data, we must use appropriate technical or organisational measures to ensure that it is appropriately protected against unauthorised access, unauthorised or unlawful processing or accidental loss, destruction or damage. In order to determine what is appropriate, we must take into account the specific security risks involved with the processing, the impact that a materialisation of these risks would have on the individuals concerned as well as the availability, suitability and disadvantages (including costs) of technical and organisational measures for securing the personal data.

3.7. Accountability

We are responsible for compliance with the principles described above and the burden of proof is on us. Therefore, it is important to document the data protection measures taken properly.

4. Transfers

Before transferring personal data to any other company or person, including to other Armacell group companies, the transferor must confirm that all requirements applicable to such a transfer are fulfilled:

- ✓ Confirm that the transfer of the personal data would be in line with the lawfulness principle according to 3.1.
- ✓ Confirm that the transfer of the personal data would be in line with the purpose of the processing according to 3.2.
- ✓ Aggregate and/or anonymise the personal data to the extent this does not interfere with the purpose of the processing.
- ✓ Personal data must not be transferred to any person who does not provide sufficient guarantees for implementing appropriate technical and organisational measures. The transferor must therefore carry out due diligence on the processor, assess the data protection risks involved and document the results.
- ✓ Before any personal data is transferred, the transferor and the processor are to enter into a data processing contract in writing or in electronic form.

The transfer from your country to another could result in the need for extra safeguards. To give you an example, resulting from the European General Data Protection Regulation (GDPR), any transfer of personal

data to countries outside the European Union requires that either the European Commission has decided that the destination territory ensures an adequate level of protection ("adequacy decision") or the transferor and the recipient have agreed the standard data protection clauses adopted by the European Commission.

Make sure you understand the local requirements for data transfers under your local data protection laws before transferring any personal information abroad.

5. Individuals' rights

Individuals have several rights, granted to them by data protection laws.

When a request from an individual for exercising any of the rights explained below has been received, it is to be forwarded promptly to the local data protection point person, who then coordinates the response to the individual. The individual's request, if justified, is to be met promptly and within one month of receipt of the request at the latest.

Individuals' rights in detail:

6.1. Right of access

If an individual requests us to do so, we must confirm to him whether his personal data is processed by us.

6.2. Right to rectification

If an individual requests us to do so, we must rectify any inaccurate personal data held on that individual.

6.3. Right to erasure

If an individual requests us to do so, we must erase all personal data held on that individual, provided that either the personal data is no longer necessary, the processing was illegal or the individual has withdrawn his consent and no other justification is available.

6.4. Right to data portability

Individuals may request personal data to be transmitted directly to another Controller in a structured, commonly used and machine-readable format.

6.5. Right to object to direct marketing

Where we process personal data for direct marketing purposes, everyone concerned has the right to object at any time. In the case of such an objection, we will cease to use his personal data for direct marketing purposes. Please make sure you understand additional local data protection requirements regarding direct marketing and to comply with them. To give you an example: in Singapore, please make sure you check the "Do-Not-Call-Registry" before preparing marketing calls.

6. Data protection impact assessment (DPIA)

Before a new personal data processing process is introduced, the prospective process owner must assess the risk to the rights and freedoms of individuals in the light of the nature, scope, context and purpose of the new process. If the risk is high according to this risk assessment, and in particular if the new process involves processing sensitive personal data on a large scale, the process owner must carry out an assessment of the data protection impact before the new process is introduced. The process owners consult with the Data Protection Officer on this.

7. Data protection by design and default

Technical and organisational measures play a key role in data protection. Wherever we process personal data, the technical and organisational measures must be designed to implement the data protection principles and integrate the data protection safeguards into our processes by default. For example, the software we use for processing personal data must be designed to automatically erase any personal data that we know will no longer be needed after a certain point of time.

8. Data Protection Officer

Armacell has a Data Protection Officer, whose contact details are published on the global Sharepoint (email: dataprotection@armacell.com). The Data Protection Officer advises the Armacell group companies as well as their directors, officers and employees of their obligations regarding the applicable data protection laws and monitors compliance with the policy and applicable data protection laws. Additionally, data protection point persons have been appointed throughout the organisation. They are responsible for supervising and coordinating the implementation of this policy with the various owners of data processing processes in their business / function.

Where you have reason to believe that applicable law prevents Armacell from fulfilling our obligations under this Global Data Protection policy, please inform the Data Protection Officer promptly. Any suspected or actual personal data breach (including loss of or damage to equipment containing personal data) must be reported to dataprotection@armacell.com or the relevant data protection point person. The Data Protection Officer handles personal data breaches with the relevant Armacell stakeholders without undue delay.

9. Training

New employees must read and understand the policies on data protection as part of their induction. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach. The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under data protection legislation.

10. Amendments

This policy may be amended from time to time. The newest version of the policy will be posted on the global Sharepoint and may also be distributed.

11. Contact

If you have any questions, comments, or requests regarding this policy, you can address them to the Data Protection Officer at dataprotection@armacell.com.

Annex 2 | Examples of personal data (non-exhaustive)

1. contact information (e.g. name, home or other mailing addresses, mobile or home contact numbers, fax numbers, personal email addresses, emergency contact information)
2. personal information (e.g. date of birth, personal identification number(s) or other social/national identification number(s), fingerprints, marital status, country of birth, nationality, citizenship, permanent residence status, race (ethnic origin), gender, religion, preferred language, bank account information, health condition(s) or other medical records, driver's license number, vehicle license plate number)
3. photographs and other visual images or recordings
4. employment, performance, compensation and benefits (e.g. employment history and letters of recommendation, hire date, position/grade, attendance, goals/objectives, performance reviews, performance and leadership ratings, salary, allowances, bonus, incentives, equity or other awards, family member/dependents' names and their relationship and dates of birth etc., grievance resolutions)
5. work permits or restrictions
6. agreements executed with Armacell
7. education and training (e.g. education level and qualifications, field and institution, competency assessments, professional licenses, certifications and awards, training courses, records and test results)
8. computer or facilities access and authentication information (e.g. identification codes, passwords, employee identification numbers)

"Special categories of personal data" can be data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It can also include genetic and biometric data (where used for ID purposes).

Annex 3 | Information to be notified to individuals

1. the name and the contact details of the Controller, i. e. that Armacell entity responsible for the Processing;
2. in case the Controller has appointed a data protection officer or in case Armacell Group has appointed a joint data protection officer, the contact details of the data protection officer;
3. the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the processing;
4. where the Processing is, by way of exception, based on pursuing a legitimate interest (3.1(d) of the Policy), the legitimate interests pursued by the Controller or by a third party;
5. the recipients or categories of recipients of the Personal Data, if any;
6. where applicable, the fact that the Controller intends to transfer personal data to a third country and reference to the existence or absence of the safeguards required for any such transfer under the GDPR and the means by which to obtain a copy of them or where they have been made available;
7. the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
8. the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the relevant individual or to object to Processing as well as the right to data portability;
9. where the Processing is based on the consent of the relevant individual (3.1(b) of the Policy), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
10. the right to lodge a complaint with a supervisory authority;
11. whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the Personal Data and of the possible consequences of failure to provide such data; and
12. the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the relevant individual.

In addition, in case the Personal Data has not been obtained from the relevant individual himself:

13. the categories of Personal Data concerned; and
14. the source from which the Personal Data originate.