GLOBAL DATA PROTECTION POLICY – THE NETHERLANDS ADDENDUM

KULICKE & SOFFA NETHERLANDS B.V. AND SUCH OTHER AFFILIATES INCORPORATED IN THE NETHERLANDS

Kulicke & Soffa

GLOBAL DATA PROTECTION POLICY – THE NETHERLANDS ADDENDUM

1. INTRODUCTION

1.1 Background to the General Data Protection Regulation

1.1.1 The General Data Protection Regulation (the "**GDPR**") is intended to offer a uniform general law for the protection of personal data in the European Union. In the Netherlands, the GDPR is supplemented by the General Data Protection Regulation Implementation Act (*Uitvoeringswet Algemene verordening gegevensbescherming,* "**Implementation Act**"). The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens,* "**Dutch DPA**") has been established to administer and enforce the GDPR. The GDPR and the Implementation Act are applicable to the following organizations:

(a) Kulicke and Soffa Netherlands Investment Holdings B.V.

(b) Kulicke and Soffa Holland Holdings B.V.

(c) Kulicke & Soffa Holdings B.V.

(d) Assembléon B.V.

(e) Kulicke & Soffa Netherlands B.V.

(f) Assembléon China B.V.

(g) Kulicke & Soffa Liteq B.V.

(individually and collectively referred to as the "**Organization**") and the Organization is committed to complying with it.

1.2 Background to the Netherlands Addendum

1.2.1 The Netherlands Addendum ("**Policy**") supplements the global data protection policy (the "**Global Data Protection Policy**") of Kulicke and Soffa Industries, Inc. and/or any of its affiliates (collectively, "**K&S**") and should be read together as one policy. Save as set out in this Policy, all other terms and principles in the Global Data Protection Policy shall continue to apply. This Policy shall apply to all K&S entities incorporated in the Netherlands and all processing of personal data by K&S in the Netherlands.

1.2.2 This Policy shall prevail in the event of inconsistency between the principles or contents stated herein and those as described under the Global Data Protection Policy.

1.3 The Netherlands Addendum Forms Part Of the Employment Contract

1.3.1 All employees and agents of the Organization must strictly comply with this Policy. For employees of the Organization, this Policy binds each employee and forms a part of the terms of the employment contract between the Organization and the employee and of the instructions given by the Organization to the employees.

1.3.2 The Organization reserves its right to amend this Policy from time to time. Any such amended Policy will similarly apply to you and become part of your employment contract with the Organization and of the instructions given by the Organization to the employees from the time of such amendment taking effect.

1.3.3 This Policy seeks to provide each employee with a broad summary overview of the requirements of the GDPR and an understanding of the GDPR's impact on operational activities. For detailed information on the obligations and exceptions under the GDPR, you may refer to the GDPR. You can find more information on the GDPR in the GDPR guide from the Dutch government:

https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming

https://www.autoriteitpersoonsgegevens.nl/

1.4 What To Do If You Are Aware Of Or Suspect A Breach of GDPR

If you have information or become aware that a breach under this Policy, Global Data Protection Policy or otherwise under the GDPR has occurred within the Organization, please report it immediately to the Data Protection Officer (you may find the contact details of such Data Protection Officer in the Global Data Protection Policy).

2. OVERVIEW OF THE GDPR

2.1 The Data Protection Obligations Applicable To Personal Data

2.1.1 With regard to dealing with personal data of any individuals, the Organization and all employees are required to adhere to the following key **data protection principles/obligations** :

(a) Lawfulness, fairness and transparency;

(b) Purpose limitation;

(c) Data minimisation;

(d) Accuracy;

(e) Storage limitation;

(f) Integrity and confidentiality;

(g) Accountability; and

(h) Individual rights management.

(the above data protection principles/obligations may be referred to in this document as the "**data protection principles**").

3. LAWFULNESS, FAIRNESS AND TRANSPARENCY

3.1 Introduction

3.1.1 Under the GDPR, personal data must be processed in a (1) lawful and (2) transparent manner, ensuring (3) fairness towards the individuals whose personal data is being processed (Article 5(1) GDPR). When processing personal data, all three elements must be met.

3.1.2 The three elements lawfulness, transparency and fairness are addressed below.

3.2 (1) ***Lawfulness***

The requirement to process personal data lawfully consists of two parts. (i) You must determine the 'lawful basis' for the processing and (ii) make sure that you process the personal data in compliance with the law.

3.3 (i) Lawful basis

3.3.1 You need to identify the specific legal ground for the processing. This is called the 'lawful basis' for processing, and there are six grounds that you can rely on depending on your purpose and your relationship with the individual.

3.3.2 Article 6 of the GDPR sets out the lawful bases for processing. When you process personal data at least one of these bases must apply at all times:

(a) Consent: the individual has given valid consent for you to process his/her personal data. The GDPR defines consent as any freely given, specific, informed and unambiguous indication of the individual's wishes;

(b) Contract: your processing is necessary for a contract with the individual. This basis also applies to the phase prior to the conclusion of the contract, provided you are acting at the request of the individual. For example, if you make a commercial proposal at the request of a customer and need to process data for that purpose;

(c) Legal obligation: the processing is necessary to comply with the law, e.g. tax or employment laws, excluding contractual obligations;

(d) Vital interests: the processing is necessary to protect the individual's life;

(e) Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a basis in law; and

(f) Legitimate interests: the processing is necessary for your or a third party's legitimate interests. Note that you cannot rely on this basis if the individual's interests overrides your legitimate interests.

3.3.3 If no lawful basis applies to your processing or personal data, such processing will be unlawful and you should refrain from such processing activity.

3.3.4 Make sure that you adequately determine and document your lawful basis before you begin processing data. You need to determine the relevant basis carefully, especially if you believe it can be based on legitimate interests, and you should not change to a different lawful basis at a later date without a good reason. This would be unfair to the individual involved, who has been informed and assumed the original lawful basis. For example, you should not change the lawful basis consent to another one because the individual withdraws his/her consent.

3.3.5 You should take into account that individuals have the right to withdraw their consent (see above Section 3.3.2 (a)) at all times and may object to the processing of personal data on the basis of a public task (see above Section 3.3.2(e)) or legitimate interest (see above Section 3.3.2 (f)).

3.4 <u>Consent in an employment context</u>

3.4.1 Extra consideration is warranted when consent is provided in an employment context due to the imbalance of power between an employer and employee.

3.4.2 Generally, the employer would have to demonstrate that consent is freely given. These are also exceptional circumstances when the employer will have to be able to demonstrate that there are no adverse consequences at all for employee, regardless of whether he/she gives consent.

3.5 (ii) Compliance with law

Lawfulness also requires that in processing the personal data the law is being fully complied with.

3.6 Special category of personal data and criminal offense data

3.6.1 The GDPR imposes severe restrictions on the use of special category of personal data and criminal offence data. This type of data requires stronger protection due to its sensitive nature. Therefore, it is prohibited to process this data unless you can rely on a legal exception.

3.6.2 Article 9 and 10 of the GDPR set out which personal data qualify as such:

(a) revealing racial or ethnic origin;

(b) revealing political opinions;

(c) revealing religious or philosophical beliefs;

(d) revealing trade union membership;

(e) genetic data;

(f) biometric data (where used for identification purposes);

(g) concerning health;

(h) concerning a person's sex life;

(i) concerning a person's sexual orientation; and

(j) about criminal allegations, proceedings or convictions.

3.6.3 In addition, note that Article 46 Implementation Act prohibits the use of the national identification numbers (*burgerservicenummer* or *BSN*), unless such use is permitted by a specific law.

3.6.4 Make sure to consult the Data Protection Officer prior to processing special category of personal data or criminal offence data (you may find the contact details of such Data Protection Officer in the Global Data Protection Policy).

3.7 International data transfers

3.7.1 Within the EU, the level of data protection is the same. This is because all EU member states must comply with the GDPR. The EU constitutes one jurisdiction within which an adequate level of protection it provided to personal data. Countries outside the EU are considered not to provide an adequate level of protection, unless the European Commission has issued an adequacy decision.

3.7.2 The main rule is that you may only transfer personal data to third countries with an adequate level of protection. Note that the term 'transfer' is interpreted broadly: the mere fact that personal data can be accessed by a party outside the EU constitutes a data transfer. For example, transfers may take place when using online IT services, cloud based services, remote access services or global HR databases.

3.7.3 If a country does not have an adequate level of protection the transfer is unlawful, unless you can rely on one of the provisions in Chapter V of the GDPR. A mechanism that is used very frequently in practice are standard contractual clauses based on the European Commission template.

3.7.4 Pay close attention when personal data is to be transferred to a non-EU country, for example due to the engagement of a cloud services provider based in the US. You must make sure to

consult the Data Protection Officer prior to permitting the transfer of personal data to a non-adequate country (you may find the contact details of such Data Protection Officer in the Global Data Protection Policy).

3.8 (2) ***Transparency***

3.8.1 The right of individuals to be informed about the collection and use of their personal data is a key principle under the GDPR. Individuals should be able to determine in advance what the scope and consequences of the processing entails. Individuals should not be taken by surprise at a later point about the ways in which their personal data has been used.

3.8.2 Articles 13 and 14 of the GDPR set out the information must be provided to individuals:

(a) Name and contact details of your organization and your representative (if any);

(b) Contact details of your data protection officer;

(c) Purposes of the processing;

(d) Lawful basis for the processing;

(e) Legitimate interests for the processing (if any);

(f) Categories of personal data obtained (if not obtained from the individual it relates to);

(g) Recipients or categories of recipients of the personal data;

(h) Details of transfers of the personal data to any third countries or international organizations (if applicable);

(i) Retention periods for the personal data;

(j) Rights available to individuals in respect of the processing;

(k) Right to withdraw consent (if any);

(l) Right to lodge a complaint with a supervisory authority;

(m) Source of the personal data (if not obtained from the individual it relates to);

(n) Details of whether individuals are under a statutory or contractual obligation to provide the personal data (if any, and if obtained from the individual it relates to); and

(o) Details of the existence of automated decision-making, including profiling (if any).

3.8.3 As a general rule, the above information must be provided to individuals at the time of the collection their personal data.

3.8.4 In the event that personal data is obtained from other sources, the above information must be provided to individuals within a reasonable period of obtaining the data and no later than one month.

3.8.5 In practice, the above information is provided by means of an online privacy notice. Make sure to refer to the policy where appropriate, e.g. on a registration form.

3.8.6 Notwithstanding the existence of the Policy, in certain situation it may be appropriate to additionally mention certain information to an individual.

3.9 (3) ***Fairness***

Fairness means that you should only process personal data in a manner that individuals would reasonably expect. You must not process the personal data in a manner which is unnecessarily detrimental or misleading to the individuals concerned.

4. PURPOSE LIMITATION

4.1 Introduction

4.1.1 You must have specified, explicit and legitimate purposes for your use of personal data, and any further use of the personal data must be compatible with those purposes. This principle is laid down in Article 5(1)(b) GDPR.

4.1.2 This principle requires that it is clear from the start why personal data is being processed and what you are going to do with this data (your purposes for the data processing). You should try to anticipate all processing purposes beforehand.

4.1.3 If you comply with your transparency obligations (see Section 3.8 above) and your documentation obligations (see Section 9 below), you are likely to automatically comply with the purpose limitation principle. This is because you must specific your purposes as a part of drafting your privacy notice (transparency) and your processing register (Article 30 of the GDPR on documentation/accountability).

4.2 Compatible purposes

4.2.1 Once your purposes are determined and you have started processing personal data, you should not just introduce a new purpose to be able to use the collected data in a new way. Such new use of the personal data that have been collected for another purpose is permitted only by exception if the compatibility test is met.

4.2.2 If you want to use the personal data already in possession for a new purpose which you did not originally anticipate, you can do so only if:

(a) the new purpose is compatible with the original purpose;

(b) you get the individual's specific consent for the new purpose; or

(c) you can point to a legal provision requiring or allowing the new processing in the public interest.

4.2.3 To assess whether the purpose is compatible with the original purpose (as set forth in Section 4.2.2 (a)), please consider inter alia the following factors: (i) any connection with the original purpose, (ii) the context in which the personal data were collected (relationship between the individual and you), (iii) the nature of the data (special personal data and/or personal data concerning criminal convictions and offences); (iv) the (possible) consequences of a disclosure; (v) the existence of appropriate safeguards (including encryption or pseudonymization); (vi) the expectations of the individual involved.

4.2.4 If you find that your new purpose is compatible, you do not need to determine a new lawful basis for the further processing. However, be aware that if you are relying on consent as a lawful basis, you have to acquire new consent to ensure your new processing is fair and lawful. When acquiring such consent, the individual involved must be made aware of the new purpose.

4.2.5 You must also make sure that you update your privacy notice so that your transparency requirement is met.

5. DATA MINIMISATION

5.1 Introduction

Pursuant to Article 5(1)(c) of the GDPR, you must ensure that personal data that is being processed is: (i) adequate - sufficient to properly fulfil the determined purpose; (ii) relevant - has a logical link to that purpose; and (iii) limited - to what is necessary: not more personal data is processed than is needed for that purpose.

5.2 Adequate, relevant and limited

5.2.1 In assessing whether you are holding the right amount of personal data, it is necessary that it is first of all clear for exactly which purposes the data is needed (see Section 4 above on purpose limitation). You must identify the minimum amount of personal data that is required to fulfil the relevant purpose. Only the data identified in that manner should be collected, and no other data.

5.2.2 Note that you should not collect of keep data on the off-chance that is may be useful in the future. Nevertheless, you may keep data in connection to a foreseeable event that may or may not actually occur.

5.2.3 Pay particular attention to the use of special category data and criminal offence data (see Section 3.6.1 above). The minimisation principle applies all the more to such sensitive data.

5.3 Periodic review

It follows from the data minimization principle that the data processing is periodically reviewed to check that the personal data is still relevant and adequate for purposes. Anything that is no longer needed should be deleted.

6. ACCURACY

6.1 Introduction

6.1.1 Article 5(1)(d) of the GDPR prescribes that personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

6.1.2 This principle is linked to the individual's right to rectification that allows the individual to have inaccurate personal data corrected. See Section 10.3 below.

6.2 Accuracy of personal data

6.2.1 Whether certain information is accurate depends on what the record that such data is included in must show and what it is used for. Note that changes to certain personal data do not have to mean that a historical record is inaccurate, as long as the record is indeed intended to be historical.

6.3 In practice

6.3.1 In practice the Organization should:

(a) take reasonable steps to ensure that processed personal data is accurate;

(b) ensure that the source and status of personal data is clear;

(c) carefully consider any challenges to the accuracy of information;

(d) consider whether it is necessary to periodically update the information and, if so, have a process in place for this; and

(e) have procedures in place to assess and timely reply to the individuals' requests for rectification.

7. STORAGE LIMITATION

7.1 Introduction

7.1.1 Article 5(1)(e) of the GDPR prescribes that personal data must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed. In other words, you cannot keep personal data for longer than you actually need it.

7.1.2 If personal data is kept for too long will it becomes unnecessary and may become irrelevant, excessive and inaccurate. There may no longer be a lawful basis for retention.

7.2 Retention policy

7.2.1 The Dutch DPA advises to determine applicable retention periods and their substantiation in a policy. This policy should be provided to the Dutch DPA upon request.

7.2.2 The GDPR does not prescribe specific retention periods. It is up to the Organization to set up retention period that are appropriate to the purposes for which the personal data is processed. The purposes of the processing must justify how long the personal data is kept.

7.2.3 A retention policy sets out standard retention periods for specific categories of information, taking into account any mandatory data retention policies prescribed by law, such as the fiscal storage obligation as set out in Article 52 of the General Act on State Taxes (*Algemene Wet inzake Rijksbelastingen*).

7.2.4 The Organization has a policy in place on retention periods and erasure of personal data. Please refer to CP-C0237 – Records Retention Policy for more information.

7.3 Job applicants

The Dutch DPA states that it is standard practice in the Netherlands to delete the data of rejected job applicants (i) within 4 weeks after the end of the job application procedure, or (ii) 1 year with the consent of the job applicant.

7.4 What is done to data that is no longer needed

You and/or the Organization must either delete or anonymise the personal data once (i) the applicable retention period expires, or (ii) before the retention period expires, provided the personal data is no longer needed.

8. INTEGRITY AND CONFIDENTIALITY

8.1 Introduction

8.1.1 Article 5(1)(f) of the GDPR requires personal data to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

8.1.2 The Organization must ensure that it has appropriate security measures in place to protect the personal data it processes. Any personal data in the Organization's possession and control must be protected by appropriate security measures.

8.2 Engagement of data processors

8.2.1 Where the Organization intends to disclose personal data to third parties that will be processing personal data on its behalf, it must ensure that a data processing agreement is entered into. The data processing agreement:

(a) Is entered into between a data controller (Organization) and data processor (e.g. a cloud service provider, hosting service provider or bookkeeper);

(b) must meet the requirements set out in Article 28(3) of the GDPR; and

(c) be concluded prior to the disclosure of personal data.

8.2.2 You must seek approval from the Organization's management or Data Protection Officer before engaging any data processor. You must also ensure that a suitable agreement is in place – obtain such agreement from the Organization's management or Data Protection Officer (you may find the contact details of such Data Protection Officer in the Global Data Protection Policy).

8.3 Personal data breaches

8.3.1 The GDPR introduces a duty to report certain personal data breaches to the relevant data protection authority and individuals involved (see Articles 33 and 34 of the GDPR).

8.3.2 Broadly speaking a personal data breach can be defined as a (security) incident that affects the confidentiality, integrity or availability of personal data. A personal data breach can fall into more than one of these three categories, depending on the circumstances. Each category is expounded below:

(a) Breach of confidentiality: an unauthorized or inadvertent disclosure of, or access to, personal data;

(b) Breach of integrity: an unauthorized or inadvertent alteration of personal data; and/or

(c) Breach of availability: an unauthorized or inadvertent loss of access to, or destruction of, personal data.

8.3.3 Examples of personal data breaches include:

(a) the loss of an unencrypted USB stick containing personal data (see specific illustration in Section 8.4.2(b) below);

(b) a cyber-attack in which personal data has been captured;

(c) an infection with ransomware in which personal data has been made inaccessible;

(d) a HR employee wrongfully sends a letter containing payroll information and personal details to the wrong employee; and/or

(e) the personal data of a large number of individuals are accidentally sent to the wrong mailing list.

8.3.4 A personal data breach may have all kinds of significant adverse effects on individuals and to the Organization.

8.4 Reporting personal data breaches: to the Dutch DPA

8.4.1 As a general rule, a personal data breach must be reported to the Dutch DPA within 72 hours after becoming aware of such personal data breach (Article 33 GDPR). Not all personal data breaches need to be reported. Personal data breaches that are unlikely to pose a risk to the

rights and freedoms of individuals are not subject to the notification requirement. Whether a personal data breach poses a risk to the rights and freedoms of individuals strongly depends on the circumstances of the matter, that must be carefully assessed.

8.4.2 Below an illustration of considerations that play a role in assessing whether a personal data breach is subject to the notification requirement (based on regulatory guidance):

(a) Personal data are already publicly available and a disclosure of such personal data does not constitute a likely risk to the individuals involved (no notification required);

(b) A lost USB stick (or another device) does not necessarily lead to a personal data breach that must be notified. As long as the personal data is encrypted with an advanced algorithm, backups of the data exist, the unique key is not compromised and the personal data can be restored in a timely matter, this personal data breach may not need to be reported. However:

i. if it turns out that the personal data on the USB has nevertheless been used by an unauthorized party, notification is mandatory; or

ii. if there is a personal data breach where there are no backups of the encrypted personal data, this could pose risks to individuals and therefore may require notification.

(c) Similarly, where a personal data breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable personal data breach, depending on the length of time taken to restore the personal data from that backup and the effect that lack of availability has on individuals.

8.5 <u>Reporting personal data breaches: to individuals</u>

8.5.1 Furthermore, it may also be necessary to notify individuals – in addition to the Dutch DPA – if the breach is likely to result in high risks for them. The threshold for communicating a breach to individuals is higher than for notifying supervisory authorities. In other words, not all breaches that must be communicated to authorities have to be automatically communicated to individuals as well.

8.5.2 A personal data breach involves a high risk when it can lead to physical, material or immaterial damage to the individuals involved. See a number of examples of these risk categories below:

(a) Physical damage: an individual's crucial medical data has been deleted, causing a risk that the individual will (temporarily) not receive the necessary care.

(b) Material damage: the risk that an individual may place orders online at another individual's expense and other forms of financial loss or identity theft or fraud.

(c) Intangible harm: the risk of discrimination, reputational damage or invasion of an individual's privacy.

8.5.3 The following contains a non-exhaustive list of examples of high risk personal data breaches (that must be notified to individuals):

(a) Discrimination: for example, in a data breach involving data on race, religion or sexual orientation.

(b) Identity theft or fraud: for example, in the event of a personal data breach involving complete passport copies or the social security number (*burgerservicenummer*) in combination with other information.

(c) A personal data breach:

i. involving special personal data;

ii. with information about personal aspects, intended to create or use profiles. In particular, if it involves profiling based on information about job performance, economic situation, health, personal preferences or interests, reliability, behavior and location;

iii. involving personal data of vulnerable groups, such as disabled people, people who are ill, children and the elderly; and/or

iv. involving a large amount of personal data and affecting a very large group of people.

8.5.4 Failure to meet the notification requirements may give rise to enforcement actions by the Dutch DPA, including substantial fines.

8.6 What to do if you are aware of or suspect a personal data breach

Under the Organization's Data Breach Management Plan, you are required to immediately contact the Data Protection Officer (you may find the contact details of such Data Protection Officer in the Global Data Protection Policy or Data breach Management Plan) in the event of an actual or suspected data breach..

8.7 Personal data breach register

8.7.1 The GDPR requires that the Organization maintains an internal register that records all personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken (Article 33(5) of the GDPR). This requirements is connected to the accountability principle. Note that registration of a personal data breach is also required if Organization's management and/or Data Protection Officer decide that there is no legal obligation to report the personal data breach to the Dutch DPA and/or the individuals.

8.7.2 The personal data breach register should at least include the personal data breaches' causes, what took place and the personal data affected. It should also include the effects and consequences of the personal data breach, along with the remedial action taken.

8.7.3 In addition to these details, it is also best to document the reasoning for the decisions taken in response to a personal data breach. Specifically, if a breach is not notified, document the justification for that decision. This should include reasons why it is considered that the breach is unlikely to result in a risk to the rights and freedoms of individuals.

9. ACCOUNTABILITY

9.1 Introduction

9.1.1 Pursuant to Article 5(2) of the GDPR, the Organization is responsible for, and must be able to demonstrate its compliance with the aforementioned principles.

9.1.2 The accountability principle imposes the requirement to have appropriate measures and records in place to be able to demonstrate compliance.

9.2 Mandatory measures

9.2.1 The mandatory measures that the GDPR specifically mentions include:

(a) maintenance of a processing register;

(b) performance of data protection impact assessment for data processing with a high privacy risk;

(c) maintenance of a register of personal data breaches that have occurred (including unreported personal data breaches); and

(d) demonstrating that an individual has actually consented to a data processing operation when you require consent for the operation.

10. INDIVIDUAL RIGHTS MANAGEMENT

10.1 Introduction

The GDPR provides individuals numerous rights in connection to their personal data that they can exercise with respect to the Organization (Chapter 3 of the GDPR).

10.2 Individual rights

10.2.1 The GDPR provides the following non-exhaustive rights for individuals:

(a) The right to be informed: individuals have the right to clear information on the use of their personal data. Generally, this information is provided in a privacy policy (see Section 3.8 above);

(b) The right of access: individuals have the right to receive, among other things, a copy of their personal data that is being processed (see Section 10.3 below);

(c) The right to rectification: individuals may have the right to have their processed personal data changed;

(d) The right to erasure: individuals may have the right to have their personal data deleted;

(e) The right to restrict processing: individuals may have the right to have less of their personal data processed;

(f) The right to data portability: individuals may have the right to have personal data transferred to another party;

(g) The right to object: individuals may have the right to object to the processing of personal data when such processing is based on legitimate interest (see example in Section 3.3.2(f) above); and

(h) Rights in relation to automated decision making and profiling (if any): individuals may have the right to a human step in the decision making process.

10.3 Right of access

10.3.1 The right of access is intended to give individuals more control over their personal data, as it allows individuals to verify which personal data the Organization holds and how it is used.

10.3.2 Upon receipt of a request for access, the Organization must provide the following information:

(a) A copy of the personal data that the individual wishes to inspect; and

(b) Information about the processing.

10.3.3 An individual has the right to inspect all or a part of the personal data that the Organization has of him/her.

10.3.4 There are different ways in which you or the Organization can meet an individual's request to access. You or the Organization may provide an individual with copies of all documents that

contain his/her personal data. Another option is to provide a requesting individual with a complete overview of personal data processed by the Organization.

10.3.5 The individual may ask to receive more information about the processing, in addition to or instead of copies of personal data. The Organization must provide the individual the following information:

(a) The purposes of the Organization's processing of personal data.

(b) What types of personal data are processed.

(c) If applicable: to which organizations the Organization transfers the personal data. This also applies to the personal data transferred to organizations in other countries or to international organizations.

(d) How long the Organization retains the personal data. If this cannot be specified precisely, you or the Organization is may instead explain the criteria used to determine a retention period.

(e) The rights available to individuals.

(f) That individuals have the right to lodge a complaint with the Dutch DPA.

(g) If applicable: from which organization the Organization have received personal data if you have not collected it yourself from the persons concerned.

(h) If applicable: on the basis of which logic you make an automated decision about an individual.

10.3.6 Much of this information is already provided in the Organization's privacy statement.

10.4 How to respond to individual requests

The Organization must reply to individual requests as quickly as possible, but no later than one calendar month starting from the day they receive the request. If the request is complex or the individual makes more than one request, the response time may be a maximum of three calendar months. Please contact the Data Protection Officer if there is an individual request.