GENERAL DATA PROTECTION REGULATION GUIDELINES

CONTENTS

1. INTRODUCTION
    1.1. Definitions

2. PRINCIPLES OF DATA PROTECTION
2.1. Lawfulness, Fairness & Transparency
2.2. Purpose limitation
2.3. Data minimisation
2.4. Accuracy
2.5. Storage limitation
2.6. Integrity and confidentiality
2.7. Accountability

3. LAWFUL BASIS FOR PROCESSING PERSONAL DATA
4. SPECIAL CATEGORIES OF PERSONAL DATA
5. INTERNATIONAL DATA TRANSFERS
6. INDIVIDUALS' RIGHTS UNDER GDPR
6.1. The Right to receive information
6.2. The Right to access
6.3. The Right to rectification
6.4. The Right to erasure
6.5. The Right to restrict processing
6.6. The Right to data portability
6.7. The Right to object
6.8. Rights in relation to automated decision making and profiling

7. APPENDIX INFORMATION SUPPLIED TO INDIVIDUALS

1. INTRODUCTION

The purpose of this document is to provide an overview of the European Union's (EU) new data protection law, the General Data Protection Regulation (GDPR). The Akvo Foundation intends to apply the standards of the GDPR organisation wide. The document includes an explanation of the legal justification ("lawful basis") for processing personal data, and the core principles of data protection and individual's rights under the GDPR.

The GDPR applies from 25 May 2018.

The GDPR aims to address the rapid changes within technology and the need to provide better data protection for individuals within the EU or where an individual's data is processed within the EU.

The GDPR applies to organisations based in the EU that process personal data. It also applies to organisations based outside the EU that offer goods or services to individuals in the EU, or that monitor the behaviour of individuals in the EU.

The GDPR emphasises the need for data processing activities to be transparent, secure and limited to what is necessary to fulfil the purpose for which the data is collected. Organisations must comply with all the principles regardless of the nature of their business and the sector in which they operate.

Fines

While there is the potential for the data protection regulations (Supervisory Authorities) in the EU to impose very large fines that are in breach of the GDPR, this is not the main aim of the GDPR & other enforcement tools could be used, such as:

- Order a company in breach of the GDPR to comply within a specified period;
- Issue warnings or reprimands to a company in breach of the GDPR;
- Impose a temporary or permanent ban on an infringing organisation's data processing activities;
- Order an infringing organisation to comply with an individual's requests'
- Communication any personal data breach directly to the affected individual(s); and
- Publish details of enforcement activity.

The Supervisory Authorities are trying to re-assure widespread concerns about their fining powers under the GDPR.

Consent

The Supervisory Authorities have recently acknowledged the widespread myth that the only way to comply with the GDPR's stringent requirements for processing consumer information is to obtain explicit consent. In fact, reliance on consent is one of six lawful bases that can be relied on, as further detailed in Section 3. Seeking consent should only be considered if no other lawful bases are available.

1.1 DEFINITIONS

Controllers are the person or organisation which determine the purpose for which, and the manner in which, personal data is processed. Throughout this document The Akvo Foundation is, in some cases, the Controller.

Processors are the person or organisation which processes personal data on behalf of the controller. Throughout this document The Akvo Foundation is, in some cases, the Processor.

Personal data means any information relating to a living individual who can be identified, directly or indirectly, from that data. This not only includes obvious identifying information such as a person's name, their date of birth or their company ID number, but also online identifiers provided by their devices such as IP addresses. Personal data encompasses all information specific to the physical, physiological, genetic, mental, economic, cultural and social identity of that person. It can include, for example, an opinion about a person.

Processing, Processed, Process means collecting, storing, analysing, using, disclosing, archiving, deleting or doing anything else with personal data.

This includes data stored systematically on systems and applications (structured data) and personal data stored or held outside of systems/applications (unstructured data).

Examples of unstructured data include:

- Shared/personal folders containing all types of documents (i.e. word, xls, Powerpoint, images, video, audio)
- Spreadsheets
- Websites/online forms
- CCTV/Recorded calls/Images
- Social media/Emails/Mobile phone - address books, messages threads/chains

Processing applies to personal data on hard copy documents if the documents are part of a filing system.

2. PRINCIPLES OF DATA PROTECTION

As mentioned above, at the heart of the GDPR are seven principles relating to the processing of personal data. These are that personal data must be:

1. Processed lawfully, fairly and transparently (**Lawfulness, Fairness and Transparency**);
2. Collected for specified, explicit and legitimate purposes (**Purpose Limitation**);
3. Be adequate and relevant (**Data Minimisation**);
4. Accurate and kept up to date (**Accuracy**);

5. Not kept longer than needed (**Storage Limitation**);
6. Kept safe and secure using appropriate measures (**Integrity and Confidentiality**);
7. That The Akvo Foundation is responsible for, and must be able to demonstrate compliance with the above principles (**Accountability**).

2.1 LAWFULNESS, FAIRNESS AND TRANSPARENCY

"Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals."

- There must be a lawful basis and business reason for processing all personal data. 'Lawful basis' has a specific meaning under the GDPR. It sets out a list of six lawful bases relation to personal data. See Section 3. At least one of these must be chosen as the legal basis for the processing in question before the personal data is collected. There is a seperate list of ten lawful bases that apply to special categories of personal data. See Section 4 for more details.
- In order to process personal data fairly and transparently, when personal data is first collected from an individual, certain detailed information must be provided to them in a clear, transparent and easily accessible form. See the Appendix to this Guidance for more information. Privacy policies will be published by The Akvo Foundation in compliance with these requirements.

2.2 PURPOSE LIMITATION

"Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;"

- A purpose must be identified and documented for each processing activity related to the personal data before it is collected.
- The individuals whose personal data is being processed must be told what the purposes are before the personal data is collected.
- Personal data should only be used for the purpose stated.
- If the purposes for which the personal data are processed are likely to change from the original purpose, there must be a procedure in place to re-assess the purpose and lawful basis of the processing activity prior to the change taking place.
- Further processing of the personal data for reasons that are compatible with the original purpose for which it is collected is permissible but can only be done if specific procedures are followed and documented, including having to inform the individuals in question first.
- Personal data should not be shared with third parties unless for its original documented purpose.

2.3 DATA MINIMISATION

"Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."

- The personal data that is collected and processed for any particular purpose must be limited to what is necessary in order for the processing activity in question to fulfil that purpose.
- All personal data must be reviewed and validated as relevant for business purposes.
- All data must be purged if irrelevant, or when no longer needed or in line with the Data Retention Schedule.

2.4 ACCURACY

"Personal data shall 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."

- Steps must be taken to ensure that accuracy of any personal data held.
- Business processes must be designed to incorporate periodic data refreshes as appropriate for the specific requirements.
- Where inaccurate personal data is identified, it must be deleted or corrected as soon as possible.
- Data processing activities should not solely be reliant on proactive updates from individuals to ensure accuracy of personal data.
- Personal data renewal should prompt for review.

2.5 STORAGE LIMITATION

"Personal data shall 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;"

- An organisation wide Data Retention Schedule and standard must be strictly adhered to.
- Data that is no longer necessary for business or legal purposes should be destroyed or deleted.
- Business processes must incorporate purging of expired or unused data.
- Third parties must be made aware of the Data Retention Schedule and subsequent data cleansing reviews.

2.6 INTEGRITY AND CONFIDENTIALITY

"Personal data shall 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 organisational measures."

- Organisational and technical information security procedures and systems must be in place to protect personal data.
- In order to comply with the GDPR's requirements relating to information security, all processes must comply with our Information Security Policy.
- Breaches of information security leading to loss of personal data not only include obvious threats like cyberattacks, but also where individuals fail to comply with internal information security policies and a loss of data occurs as a result.
- The Akvo Foundation will provide an Information Security Policy and will include the new requirements for breach reporting.

2.7 ACCOUNTABILITY

"The controller shall be responsible for, and be able to demonstrate compliance with, the principles of the GDPR."

- The seventh principle - Accountability - is an important new obligation in the GDPR compared to the previous data protection directive.
- Records must be kept in relation to all personal data processing activities in order to demonstrate compliance.
- This means that documentation of decision making relating to processing of personal data is important.

3. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

To be able to process personal data one of the following conditions must be met:

1. **Contract**: where the processing is necessary for the performance of a contract. For example, a customer name and address to supply goods or services requested, or an employee's bank details for payroll purposes under an employment contract. The word 'necessary' is interpreted strictly: if the contract

could be performed without the personal data, then the processing is unlikely to be necessary.

2. **Compliance with a legal obligation**: where the processing is necessary for The Akvo Foundation to comply with a legal obligation under Dutch and EU law.

3. **Legitimate interests**: The Akvo Foundation can process personal data on the basis of a genuine and legitimate reason, so long as the processing is not prejudicial to the rights and interests of the individuals in question.

   Examples of legitimate interests given in the GDPR include: fraud prevention, transferring personal data within a group of companies or processing of personal data strictly necessary and proportionate for the purposes of ensuring network and information security.

   Where The Akvo Foundation does not have a contractual or legal obligation as a lawful basis to process personal data it is likely to look to rely on the legitimate interests condition.

   In choosing legitimate interests as the lawful basis for processing personal data, two points should be kept in mind: i) the individuals in question have to be informed what the legitimate interest is (see the Appendix to this Guidance); and (ii) individuals have the right to object to processing that relies on the legitimate interests condition.

4. **Consent:** where the individual has given consent for their personal data to be processed for a specific purpose.

   The GDPR defines consent as a freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or a clear affirmative action (such as ticking a box), signifies agreement to the processing of his or her personal data. Failure to respond does not amount to consent. Consent can be withdrawn at any time (and this must be easy to do) and the individuals in question must be informed of this at the outset (see the Appendix). Wording seeking consent must be prominent and separated from other text, it cannot be buried in the small print of the contract, for example.

   Consent should only be considered if there is no other lawful basis e.g. to use sensitive personal data, children's data or for general marketing. No preticked boxes are permitted and implied consent is not sufficient. There is a higher threshold of explicit consent relating to special categories of personal data. See Section 4.2.

   In line with the recommendations from various people in the legal field as well as IT security field, The Akvo Foundation should not rely on consent as a lawful basis for processing.

5. Vital interests: personal data can be processed if it is necessary to protect someone's life. This could be the life of the individual or someone else.

   Vital Interests is only likely to be used for Crisis Management.

6. A Public Task: if you need to process personal data to carry out an official function or a task in the public interest - and there is legal basis for the processing under Dutch and EU law. This is not a likely option for The Akvo Foundation.

4. SPECIAL CATEGORIES OF PERSONAL DATA

1. Particular care should be taken in relation to the processing of personal data in the following, sensitive or special categories (Special Categories of personal data):

   - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
   - Genetic data and biometric data processed for the purpose of uniquely identifying an individual;
   - Personal data concerning an individual's health, sex life or sexual orientation; and
   - Personal data relating to criminal convictions and offences or related security measures.

2. In particular, Special Categories of personal data should not be processed except where:

   - The individual has given his or her explicit consent to the processing for one or more specified purposes;
   - The processing is necessary for the purposes of performing obligations or exercising specific rights under employment, social security or social protection law;
   - It is necessary for a legal claim;
   - A member state of the EU has passed a law permitting the processing;
   - It is necessary to protect the vital interests of the individual;
   - Processing is carried out by a foundation or not-for-profit organisation;
   - The personal data has been made public by the individual;
   - Reasons of public interests in the area of public health; or
   - Archiving purposes in the public interest.

5. INTERNATIONAL DATA TRANSFERS

1. Personal data may only be Transferred outside the European Economic Area (the EU, plus Iceland, Liechtenstein and Norway) where one or more of the following applies:

    - Where the Transfer is to a country or other territory which has been assessed by the EU Commission as ensuring an adequate level of protection for personal data;
    - Where the individuals whose personal data are being processed have been given their explicit consent to the Transfer taking place; or
    - Where The Akvo Foundation has approved the Transfer on the basis that it is compliant with the GDPR and other applicalbe laws.

2. For the purposes of this Guidance, a Transfer is any transfer of Personal Data. this includes arrangements through which a person outside the EEA has remote access to Personal Data stored within the EEA.

6. INDIVIDUALS' RIGHTS UNDER GDPR

Individuals have rights under the GDPR in relation to their personal data, these are the rights of:

1. Information
2. Access
3. Rectification
4. Erasure
5. Restriction of Processing
6. Data Portability
7. Objection to processing; and
8. Rights in relation to Automated Decision Making and Profiling

Although these rights are very powerful, The Akvo Foundation does not expect to handle many external requests invoking them as we are a not-for-profit organisation who deal mainly with other organisations rather than individuals, and we are mainly Processors of data rather than Controllers.

6.1 THE RIGHT TO RECEIVE INFORMATION

- Individuals must be informed of the way their personal data is going to be used, processed and stored including whether it is going to be passed to any third parties and/or outside the EEA.
- All information detailed in the Appendix to this Guidance (Information supplied to individuals) must be provided to the individual before any personal data is collected.

6.2 THE RIGHT OF ACCESS

- Individuals have the right to submit a Subject Access Request (SAR) which is a request for information held on themselves and the way their personal data is being used and/or stored.
- The identity of the requestor must be verified and the request validated before fulfilling a SAR.
- SARs must be fulfilled within one month of verifying the identity of the requestor.
- The Akvo Foundation must contact the requestor as soon as possible, not more than 3 days after receiving the request to validate the identity of the requestor.
- The one month deadline applies from the day the requestor provides the information to validate their identity. If the request is complex and numerous the period can be extended to two months.

6.3 THE RIGHT TO RECTIFICATION

- Individuals have the right to update personal data held on them that is inaccurate or incomplete.
- The Akvo Foundation's processes must incorporate the capability to verify an individual's identity and implement requested corrections across all systems and data backups.

6.4 THE RIGHT OF ERASURE

1. Individuals have the right to request deletion of their personal data i.e. to be forgotten. This is not necessarily an absolute right. There are a number of factors to consider when verifying whether an individual's request to have their personal data deleted from a system must be complied with. For example, The Akvo Foundation has a legal duty to retain data for specific time periods, therefore if the request falls within the time period the request can legitimately be refused. See further guidance below.

2. The most relevant grounds on which an individual is likely to request erasure of their personal data are where:

    - The data is no longer needed for the purpose it was originally collected for;
    - The individual objects to processing that is based on the legitimate interests condition and there are no overriding legitimate grounds for the processing, or other lawful grounds for it; or
    - The individual withdraws consent when consent was being used as the lawful basis for processing.

    The Akvo Foundation's processes must incorporate the capability to verify an individual's identity and implement deletion across all systems and backups where the request is valid.

    Internal processes must incorporate the individuals' right to request changes (Right to Rectify) or erasure (Right to be Forgotten), and notification to third parties of these requests.

3. The right can be refused when:

    - It is made on the basis that the data is no longer needed, but the data has not expired according to the timeframes set out in the Data Retention Schedule.
    - There is a legal obligation to retain the data beyond the period listed in the Data Retention Schedule; or
    - The data is part of a legal claim.

6.5 THE RIGHT TO RESTRICT PROCESSING

Individuals have the right to restrict processing of personal data i.e. personal data may be stored but no further processing may take place.

The right applies:

- Where individuals contest accuracy of the personal data;
- Where individuals disagree with the lawful basis for processing; or
- When the personal data is no longer needed but the individual requires the data to establish, exercise or defend a legal claim.

The Akvo Foundation's processes must incorporate the capability to capture and flag any data restrictions as requested and inform the individual when a restriction on processing is lifted.

6.6 THE RIGHT TO DATA PORTABILITY

Individuals have a limited right to obtain and reuse their personal data for their own purposes across different services. Individuals have the right to move, copy or transfer personal data easily from one company to another. It is unlikely that data portability requests will be received at The Akvo Foundation. However, Akvonauts should be aware that the right exists.

This right applies when three conditions are met:

- Where the individual has provided the personal data to The Akvo Foundation;
- Where the processing is based on the individual's consent or to fulfil a contract; and
- When processing is carried out by automated means.

6.7 THE RIGHT TO OBJECT

Individuals have the right to object to processing of their personal data based on legitimate interests and/or to using their information for direct marketing. The 'legitimate interest' lawful basis is described in Section 3 of this guidance document. It should be noted that the right to object to processing based on legitimate interests, is not an absolute right and in some limited circumstances may be overridden as stated below:

- Individuals must be informed of their right to object "at the point of first communication" and in privacy notices.
- Processing of personal data for direct marketing purposes must stop as soon as an objection is received. There are no exemptions or grounds to refuse.

1. The right applies

    - To all automated processing activies; and
    - It should be noted that if processing activities take place online, individuals must be offered a way to object online.

2. The right to object based on legitimate interest can be refused:

    - If it can be demonstrated there are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individuals; or
    - The processing is for the establishment, exercise or defence of legal claims.

6.8 RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING

GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

For the purposes of the GDPR, automated profiling is any form of automated processing intended to evaluate personal aspects of an individual to predict an outcome.

1. Automated decision-making processes must be identified and must incorporate the capability to provide human intervention on request so that:

    - The individual's point of view can be expressed; and
    - An explanation of the decision is received and can be challenged e.g. a credit risk report, where an individual has the right to provide further information which may affect the outcome of the automated report.

2. This right applies when:

    - A decision is based on automated processing; and
    - The decision has a legal or significant effect (e.g. loan application, job application) on the individual.

3. This right can be refused if:

    - The lawful basis of the processing is that of necessity to perform a contract (see section 3);
    - It is authorised by law (for example, for the purposes of fraud or tax evasion prevention;
    - It is based on explicit consent; or
    - The processing does not have a legal or similar effect on the individual.

4. Examples of Automated Profiling are as follows:

    - Performance at work (Job applications / Performance reviews);
    - Economic situation (credit risk)
    - Health;
    - Personal preferences;
    - Reliability;
    - Behaviour;
    - Location; and
    - Movements.

5. Safeguards

   Automated processes must be fair and transparent by:

   - Providing meaningful information about the logic involved;
   - Using appropriate mathematical or statistical procedures;
   - Implementing appropriate technical or organisational measures to minimise the risk of errors and correction of incorrect information; and
   - Securing personal data that is proportionate to the risk to the interest and rights of the individuals and with no discriminatory effect.

The Akvo Foundation be setting up the necessary forms and contact options to capture and respond to these requests.

7. APPENDIX INFORMATION SUPPLIED TO INDIVIDUALS

What information must be supplied?	Personal data obtained directly from individual	Personal data not obtained directly from individual
Identity & contact details of controller & where applicable, the controller's representative & the data protection officer	✓	✓

Purpose of the processing & the lawful basis for the processing	✓	✓
The legitimate interests of the controller or 3rd party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to 3rd parties/other countries & safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of individual's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from & whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation & possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling & information about how decisions are made, the significance & the consequences	✓	✓
When should information be provided?	At the time the personal data is collected	Within a reasonable period of having collected the personal data (within one month) If the personal data is used to communicate with the individual, at the latest, when the first communication takes place; or If the disclosure to another recipient is envisaged, at the latest, before the personal data is disclosed.