GDPR Compliance Statement

From 25 May 2018 the General Data Protection Regulation (GDPR) will apply in the entire EU. These new privacy rules apply to every organisation processing personal data from individuals located in the EU, including Credproof Inc. ("Credproof") and its customers. The GDPR replaces and extends the scope of the former EU directive and its national implementation laws. The fine-thresholds for non-compliance have also been increased considerably.

The aim of this Statement is to:

- Inform you about the GDPR;
- Inform you on what Credproof has done and will continue doing to comply with the GDPR; and
- Help you comply when using Credproof's products and services;

About the GDPR

The GDPR is widely regarded as one of the most important pieces of legislation applicable to the digital sector in the EU, if not the most important.

A core value of the GDPR is that **human beings ('data subjects') should have control over their own personal data**. When an organisation controls personal data (any information that says something about, or can be used to identify, a human being), the organisation must comply with the following **key obligations**.

About this Statement

- All processing of personal data must comply with **fundamental principles**, such as lawfulness, fairness, transparency, purpose limitation, data

minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability);

- All processing of personal data must be founded on a valid and applicable **legal basis listed in the GDPR** (e.g. if the data subject has given **informed consent**, or if processing is **necessary** to **perform a contract with the data subject**);

- Data subjects must be informed about **what information is processed about them,** why (including the applicable legal basis), for how long, and how it is secured;

- The following **rights of data subjects** must be complied with, and data subjects must be explicitly informed about their rights to:
    1. obtain **access** to the data processed about them;

    2. have their data **corrected**, **erased** or **restricted** when incorrect or no longer necessary;

    3. **object** to certain processing of their data;

    4. **take their data** with them to another provider;

    5. **not be subjected to profiling** and **automated decision-making** without their express consent;

    6. **complain** to a supervisory authority about the way their personal data is processed;

- Organisations processing personal data more than just occasionally must **keep an up to date record** (overview) of the kinds of personal data they process, about what kinds of data subjects, why (which applicable legal basis), for how long, using which data processors, and where;

- Organisations whose core activities revolve around processing personal data must appoint a **data protection officer (DPO)**, a privacy expert who is responsible to help them comply with the GDPR and should be consulted on all important privacy matters;

- For **new and riskier forms of personal data processing**, a **data protection impact assessment (DPIA)** must be performed first;

- **Personal data must be appropriately secured** against accidental or unlawful destruction, loss, alteration and unauthorised disclosure or access;

- In the event of a **personal data security breach**, the supervisory authority and/or affected data subjects must be **notified**;

- In **designing systems** used to process personal data, **privacy** should be implemented **by design and by default**;

- Where another party (a 'processor') is contracted to process personal data on the organisation's behalf, a **data processing agreement** is required;

- Processing of **personal data may not be outsourced to countries outside the EEA, unless** specific appropriate **safeguards** are in place, such as contractual **model clauses, binding corporate rules**, or a specific arrangement such as the **EU-US Privacy Shield**.

Important terms and definitions of the GDPR

"Personal data"

GDPR art 4(1)

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or

more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

This definition is very broad: all information relating to an identified or identifiable natural person (called the ‘data subject’). Importantly, this does not only cover ‘personally identifiable information’ (knows as ‘PII’ mostly in US jurisdictions) which directly identifies a person, such as names, addresses, and telephone numbers; but also IP-addresses, information on personal interests, and much of the information stored and read via cookies. Even if someone’s name is not known, a customer profile still contains personal data.

"Processing"

GDPR art 4(2)

‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

This definition is also very broad. ‘Processing’ is every operation that is carried out using personal data: not only viewing or modifying the data, but also its mere storage, transfer, and even its deletion.

"Controller"

GDPR art 4(7)

‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. In essence, the controller is the party who determines why and how personal data is processed. This often is a party who has a contract with individual persons to provide products or services to them.

"Processor"

GDPR art 4(8)

‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
The processor is the party who is engaged by the controller to process personal data on behalf of the controller.

What Credproof has done and continues to do to comply with the GDPR

Credproof as processor

Certain obligations under the GDPR are applicable to ‘controllers’ (the party who determines why and how personal data is processed), whereas other obligations apply to ‘processors’ (the party who processes personal data on behalf of the controller). Credproof’s products and services are intended to help customers manage the digital identities of their users. As such, Credproof processes personal data about the (potential) users of customers on the latter’s behalf, and therefore qualifies as a processor in this respect.

Credproof’s **data processing agreement** regulates Credproof’s processing of personal data of your (potential) users, and helps you to demonstrate compliance with the GDPR when using Credproof’s products and services.

Credproof as controller

Credproof also processes personal data about their customers themselves and their representatives and employees. In this context, Credproof determines the purposes and means of the processing activities, and therefore qualifies as controller.

Credproof’s **privacy policy** regulates the processing of your own personal data, and of your employees or colleagues using, purchasing or administrating Credproof’s products or services, and provides you with all the required information and data subjects’ rights.

Data processing principles

Processing of personal data must comply with the GDPR's fundamental principles. We do our utmost, and will continue doing so, to implement these data processing principles into the very core of our products, services, and organisation.

Lawfulness, fairness and transparency

We only process personal data when we deem this necessary for a legitimate purpose under the GDPR, and we do our utmost to provide complete yet concise and easily accessible and understandable information about all of our personal data processing activities.

Purpose limitation

We only use personal data for the purposes for which they were collected, as described in our privacy policy and data processing agreement. For example, Credproof will not use e-mail addresses collected to send advertisements or other forms of unsolicited messaging.

Data minimisation

We only use personal data for the purposes for which they were collected, as described in our privacy policy and data processing agreement. For example, Credproof will not use e-mail addresses collected during a booking to send advertisements or other forms of unsolicited messaging.
We do not process more personal data than we deem strictly necessary to provide you with optimal products and services. We do not combine any personal data we have gathered in providing our products and services to you, with any other personal data we may have obtained elsewhere, unless we have first obtained your specific, explicit, informed consent. If your agreement with Credproof has ended, we return your data to you upon your request, and/or it will be deleted from Credproof's servers.

Accuracy

The principle of accuracy also is a requirement for controllers. It means that data should be kept up to date where necessary and should always be as accurate as possible.

Storage limitation
Personal data should not be kept longer than necessary to reach the predefined goals. This means that if personal data is no longer needed, it should be securely deleted.

Integrity and confidentiality
To protect, secure and preserve personal data, controllers should implement an information security framework. Credproof takes adequate technical and organisational measures to protect personal data, as explained in our security documentation (see below).

Accountability
The principle of accuracy also is a requirement for controllers. It means that data should be kept up to date where necessary and should always be as accurate as possible. If you need us to help you in correcting certain data about your users or yourself, please let us know and we will provide all the help we can.
We have drafted the present document specifically to help demonstrate our compliance with the above principles, and also to help you demonstrate your compliance if you decide to purchase our products and services.

We have also drafted and adopted several relevant internal documents and policies, helping us to demonstrate that we actually put the principles and obligations of the GDPR into practice. More information about this is provided further below.

Lawful basis for processing personal data

Article 6 of the GDPR provides the valid legal grounds for processing personal data. This list is exhaustive, meaning that these grounds listed are the only valid legal grounds, and at least one of these grounds must always be valid and applicable to justify any processing of personal data.

1. Informed consent;
2. Performance of a contract;

3. Compliance with a legal obligation;
4. Vital interests of the data subject;
5. Performance of a public task;
6. Legitimate interests pursued by the controller

When you request us to deliver products or services, or request us to provide relevant information, we process your information to perform a contract with you, or to make the appropriate preparations for doing so.

When you have concluded an agreement with us to use our products and services, we process personal data of your (potential) users in order to perform our agreement.

Our measures demonstrating GDPR compliance

Besides the present compliance statement, the following documentation and policies have been adopted to comply with the GDPR and to be able to demonstrate GDPR compliance.

- our processing purposes;
- the categories of data subjects we process information from;
- the types of personal data (e.g. name, etc);
- Data subjects' rights (e.g. correction, erasure, restriction, objection, complaints)

External privacy policy

We have thoroughly reviewed our privacy policy in order to provide all the relevant information required by the GDPR. This includes information about the following:

- a description of the applicable processing activities;
- applicable purposes and instructions;

- measures for security and confidentiality;
- applicable sub-processors and procedure for engaging another
- (sub-)contractor;
- personal data breach notification obligations;
- assistance obligations to help ensure data subjects' rights;
- returning or deleting personal data upon termination;
- audits and inspections.

A data processing agreement for Credproof customers can be requested by emailing privacy@credproof.com

Data processing agreement

Our data processing agreement has been drafted by legal specialists in order to incorporate all that is required by the GDPR. For example, our DPA contains provisions concerning:

Security documentation

We have implemented a process to regularly assess and update our security measures, and we have documented our current security measures. Where relevant and possible, we implement encryption and pseudonymisation to protect personal data and enhance privacy, as suggested by the GDPR. In order to prevent having to update our documentation too often and moreover to safeguard to prevent that information about our security can be abused, our security documentation is focused on providing a high-level overview of security measures, and not on providing detailed (technical) descriptions.

Internal record of processing activities

Under the GDPR it is mandatory for both data controllers and data processors to keep a record of processing activities. Credproof keeps a record of whose personal data is being processed, and for which purposes. We also document to whom we transfer the data, and which security measures we have taken to protect the data.

Internal privacy policy

We have drafted and adopted an internal privacy policy which outlines to employees how they must handle personal data for Credproof, and also how their own personal data is handled by Credproof.

Privacy by design and by default in our products and services

When (further) developing our products and services, we take privacy into account as one of the main requirements. The standard settings of our service allow for processing of a minimum amount of data.

Data Protection Officer

In some cases, the GDPR requires for a Data Protection Officer (DPO) to be appointed. Credproof has appointed a DPO, who advises Credproof on privacy matters.

Data Protection Impact Assessment

If Credproof, in the future, will plan to carry out processing of personal data which entails a high risk for data subjects (such as large-scale processing of sensitive data, or automated decision-making based on profiling), it will assist its customer in carrying out any required Data Protection Impact Assessment before starting the provision of these services.

Appropriate safeguards for international transfer

The GDPR requires appropriate safeguards for the transfer of personal data outside the European Economic Area (EEA), which includes all EU countries and non-EU countries Iceland, Liechtenstein and Norway. When we store data outside the EEA, we make sure to conclude EU Standard Contractual Clauses with the relevant third party, or make sure that the relevant US-based service provider is Privacy Shield certified.