# Data protection policy

## Part I: Policy details

### 1. What does this policy cover and who is covered?

1.1. CreoPlan Ltd takes the protection of Personal Data seriously. Personal Data means any information from which a living individual (called a Data Subject) can be identified. It does not include information which has been anonymised. Personal Data can come in many forms: at its simplest it may be a name, address, and telephone number, but it can include a wide range of matters such as an individual's opinion or their preferences. Under GDPR an IP address is also considered to be Personal Data.

1.2. As a business, we are required to comply with the UK's Data Protection Laws and we are fully committed to ensuring that compliance. The protection of Personal Data also has a big impact on our reputation as a business. As you are covered by this policy and your contract with us requires you to comply with it, you are also obliged to ensure that all Personal Data that you may handle, or to which you may have access as you carry out your contracted duties, is properly protected.

1.3. This is an internal policy that sets out how we handle the Personal Data of any individuals we deal with. It applies to all Personal Data held about our customers and potential customers, suppliers, business contacts and any other individuals who we deal with in the course of our business. It also applies to how we handle the Personal Data of our staff and other workers and to the Personal Data of our shareholders.

1.4. CreoPlan Ltd keeps this data protection policy under regular review, so it may be updated from time to time.

### 2. Key terms and definitions

2.1. Data protection law contains a lot of technical terms. To make life easy, we've defined them upfront here so that you can get used to them.

**Automated Decision-making:** a decision made by automated means, without any human involvement.

**Consent:** the freely-given, specific, informed, and unambiguous consent of a living individual to whom the Personal Data relates (a Data Subject) to the Processing of their Personal Data. This consent must have been indicated by clear and affirmative action.

**Data Controller**: the organisation or person responsible for deciding how Personal Data is collected, stored, and Processed.

**Data Processor**: a Data Controller may appoint another organisation or person to carry out certain tasks in relation to the Personal Data on behalf of, and on the written instructions of, the Data Controller. These tasks might include, for example, hosting of a website, running of marketing mailshots, and providing payroll services.

**Data Protection Laws**: the Data Protection Act 2018 and the General Data Protection Regulation ((EU) 2016/679) (the GDPR) and such other laws as may be applicable from time to time, including any replacements.

**Data Subject:** a living individual to whom the Personal Data relates.

**EEA:** the European Economic Area (and the countries comprised in it).

**GDPR:** the General Data Protection Regulation ((EU) 2016/679).

**ICO:** the Information Commissioner's Office.

**Personal Data:** any information from which a living individual (a Data Subject) can be identified. It does not apply to information that has been anonymised. Personal Data can come in many forms: at is simplest it may be a name, address, and telephone number, but it can include a wide range of matters such as an individual's opinion or their preferences. Under GDPR, an IP address is also considered to be Personal Data.

**Process (or similar words)**: any activity (or series of activities) in relation to Personal Data, which can include collection, recording, retrieval, storage, consultation, use, alteration or amendment, transmission, disclosure, or deletion or destruction of the Personal Data.

**Profiling:** automated Processing of Personal Data to evaluate certain things about a Data Subject (such as to analyse or predict aspects of that Data Subject's personal preferences, behaviour, or location).

**Special Categories of Personal Data:** under GDPR, these are certain more sensitive types of Personal Data. This is any information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation, or anything which is health, genetic, or biometric information.

## Part II: Data protection responsibility

### 1. Compliance and compliance officers

1.1. CreoPlan Ltd is required to comply with Data Protection Laws. Our directors, employees, workers, contractors, and others in similar capacities are also required to comply with these laws. You must ensure that you read and understand this policy so that you know what you must and must not do, and what is required from you in relation to the handling and use of any Personal Data, in order for you and CreoPlan Ltd to comply with the Data Protection Laws.

1.2. If you do not comply with this policy, we may take disciplinary action against you.

1.3. We have appointed Simon Davison as our Data Protection Officer (referred to in this policy as the **DPO** ) who has overall responsibility for overseeing the CreoPlan Ltd's compliance with Data Protection Laws. You can contact them in the following ways:

a. Simon@creoplan.co.uk

1.4. You should contact the **DPO** if you have any questions or concerns about data protection, Data Protection Laws, this policy, and any breach of the laws or this policy.

1.5. This policy also indicates specific situations when you must contact the **DPO** , for example, when there is a Personal Data breach, before you use or handle data in a new way, or when you receive any request from an individual exercising any of their rights under the Data Protection Laws.

## 2. The Accountability Principle

2.1. CreoPlan Ltd is required to comply with the Data Protection Laws and to demonstrate its compliance with the Data Protection Laws (this is referred to in Data Protection Laws as the **Accountability Principle**).

### Required measures

2.2. We are required to put in place measures to meet the requirements of the Accountability Principle and these measures include:

a. adopting this Data Protection Policy;

b. providing regular training to staff on Data Protection Laws and this Data Protection Policy (and other related policies, as relevant);

c. implementing a 'data protection by design and default' approach (see Part VI, Section 1);

d. having in place written contracts with any third parties who Process Personal Data on our behalf (see Part IV, Section 3.4);

e. recording and maintaining documentation that sets out in full CreoPlan Ltd's Processing activities (see below in this Part);

f. implementing appropriate security measures (see Part IV, Section 1);

g. recording and, where necessary, reporting Personal Data breaches (see Part V, );

h. conducting data protection impact assessments for uses of Personal Data that are likely to result in high risk to Data Subjects' interests and where required by Data Protection Laws (see Part VI, Section 2);

i. conducting regular reviews and, where necessary, implementing updates to the above measures.

### Record-keeping

2.3. The **DPO** has in place a central written record that explains in full all of the company's Processing activities.

2.4. Where we are a Data Controller, these records must include (as a minimum):

a. our name and contact details and those of any joint Controllers;

b. (where applicable) the name and contact details of any DPO appointed;

c. why the Personal Data is being processed;

d. a description of the categories of people covered (the Data Subjects);

e. a description of the categories of Personal Data involved;

f. a description of the categories of recipients to whom the Personal Data will be disclosed (including details of transfers of Personal Data outside of the EEA, the details of the third country or organisation, and the safeguards in place);

g. details of retention periods – i.e. for how long the data will be kept; and

h. a description of the technical and organisational security measures that CreoPlan Ltd has put in place to protect the Personal Data.

2.5. These records can only be kept up to date if the **DPO** is kept fully informed about our Processing activities. So, where you or your team/department intend to carry out any new Processing, disclose Personal Data to a new third party, transfer Personal Data abroad, or do any of the other matters that may affect the records or other documentation that CreoPlan Ltd has in place, you should contact the **DPO** before carrying out these activities, to ensure that all documentation can be updated and also that, as a business, we remain compliant with Data Protection Laws.

# Part III: Data protection principles

## 1. Overview

1.1. The GDPR has six main principles for the Processing of Personal Data. These are:

1.1. The GDPR has six main principles for the Processing of Personal Data. These are:

a. Personal Data must be Processed lawfully, fairly, and transparently (**Principle 1**);

b. Personal Data must only be collected and Processed for specified, explicit, and legitimate purposes (**Principle 2**);

c. Personal Data must be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is Processed (**Principle 3**);

d. Personal Data must be accurate and where necessary, kept up to date (**Principle 4**);

e. Personal Data must not be kept for longer than is necessary for the purposes for which it is Processed (**Principle 5**);

f. Personal Data must be Processed securely, and appropriate measures must be taken to protect against unauthorised or unlawful Processing and against all accidental loss, destruction, or damage to the Personal Data (**Principle 6**).

1.2. We have set out below more detail about each of the above principles and how they apply to you and CreoPlan Ltd.

## 2. Lawfulness, fairness, and transparency (Principle 1)

2.1. Personal Data must be Processed lawfully, fairly, and transparently.

2.2. CreoPlan Ltd must only collect and Process Personal Data where it has a 'lawful reason' for doing so. Those lawful reasons are set out in the GDPR and include:

a. CreoPlan Ltd has the Consent of the Data Subject to Process their data for specific purpose(s);

b. Processing is necessary in order for CreoPlan Ltd to perform its obligations in relation to an existing contract or a contract it is about to enter into with the Data Subject;

c. Processing is necessary for a legal obligation that CreoPlan Ltd is subject to;

d. Processing is necessary to protect the vital interests of the Data Subject or another person;

e. Processing is necessary in CreoPlan Ltd's or a third party's legitimate interests, but only so long as those legitimate interests do not override the fundamental rights and freedoms of the Data Subject.

2.3. Where CreoPlan Ltd is relying on Consent as the lawful reason, there are specific requirements that must be complied with:

a. the Consent itself must provide the Data Subject with sufficient information to ensure that they are informed and understand what they are being asked to consent to;

b. the Consent must be by way of positive action – that is the Data Subject must positively agree. Silence and pre-ticked boxes do not count as Consent;

c. any request for Consent must be separate to any other matters (for example, it should not be a condition of a contract or terms and conditions);

d. records of Consent must be kept (for example, you must record when and how the Data Subject consented and what they were told).

2.4. The GDPR requires CreoPlan Ltd to keep a record of the lawful reason(s) it relies on to Process Personal Data. If you plan on carrying out Processing for a new purpose, if you are not sure which lawful reason applies to the Processing, or if you need help with ensuring that any Consent is GDPR-compliant, contact the **DPO** .

2.5. If CreoPlan Ltd Processes any Special Categories of Personal Data, it must identify the relevant lawful reason for Processing (as set out above) and it must also identify a separate condition for Processing those Special Categories of Personal Data. Those separate conditions include (among others):

a. the Data Subject has provided their explicit Consent;

b. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of CreoPlan Ltd or of the Data Subject, under employment and social security and social protection law;

c. Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;

d. Processing relates to Personal Data that are manifestly made public by the Data Subject;

e. Processing is necessary for the establishment, exercise, or defence of legal claims; and

f. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services.

2.6. If you are intending to collect any Special Categories of Personal Data, are not sure which of the separate conditions applies, or if you need help with ensuring that any Processing of Personal Data is GDPR-compliant, contact the **DPO** .

2.7. As part of the fairness element of Principle 1, CreoPlan Ltd should only Process Personal Data in ways that a Data Subject would reasonably expect.

2.8. As part of the transparency element of Principle 1, where CreoPlan Ltd is acting as Data Controller, it must provide Data Subjects with certain information about its use of their Personal Data. This is usually done via a 'privacy notice'. CreoPlan Ltd is required to comply with the following:

a. the privacy notice must be in writing, clear, concise, transparent, and intelligible using clear and plain language (i.e. no jargon);

b. the privacy notice must cover all the requirements required by the Data Protection Laws;

c. where we collect the Personal Data directly from the Data Subject we must provide the privacy notice to the Data Subject at the point of first collection of the Personal Data;

d. where we receive Personal Data indirectly (for example, from a third party or from a public source), we must provide the privacy notice to the Data Subject within a reasonable time of receiving the Personal Data (and no later than one month after receiving it) or, if earlier than that month deadline, at the point of first communication with the Data Subject or before the Personal Data is disclosed to a third party.

2.9. CreoPlan Ltd already has in place several privacy notice(s) to cover its current activities. These are available from Simon Davison. You should check these very carefully to see if they are suitable; and, if they are not or you are not sure if they are suitable or if you have any questions in relation to them, you should contact the **DPO** for assistance and advice.

### 3. Purpose limitation (Principle 2)

3.1. Personal Data must only be collected and Processed for specified, explicit, and legitimate purposes.

3.2. You must not Process any Personal Data for any purposes that are incompatible with the original purposes that were disclosed (via a privacy notice) to the Data Subject when the Personal Data was first collected.

3.3. If you do intend to Process the Personal Data for further purposes, prior to taking any actions you must first speak to the **DPO**, who will be able to advise you whether it is possible and, if so, what steps need to be taken to comply with Data Protection Laws. The **DPO** will also need to update the documentation that CreoPlan Ltd has in place relating to the Processing of Personal Data to cover the new purposes.

### 4. Data minimisation (Principle 3)

4.1. Personal Data must be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is Processed.

4.2. You should only collect the Personal Data you actually require to carry out your work. You should not collect anything beyond this.

4.3. You must not Process Personal Data for any reason other than to carry out your work.

### 5. Accuracy (Principle 4)

5.1. Personal Data must be accurate and, where necessary, kept up to date.

5.2. You must ensure that when Personal Data is collected that it is accurate. You should check the accuracy of the Personal Data regularly occasions. If Personal Data is not up to date or is inaccurate, you must update the Personal Data or erase it without delay, after taking into consideration the purposes for which the Personal Data was collected.

### 6. Storage limitation (Principle 5)

6.1. Personal Data must not be kept for longer than is necessary for the purposes for which it is Processed.

6.2. You must not keep Personal Data from which a Data Subject is identifiable for longer than is necessary for the purpose(s) for which the Personal Data was originally collected. Those purposes would also include any legal, accounting, regulatory, or similar obligations we have to retain the Personal Data.

6.3. CreoPlan Ltd has in place retention policies that set out retention periods for different types of data and information (including Personal Data) with which you must comply.

6.4. Where Personal Data is no longer required it should be deleted or destroyed from our systems and all paper copies of the Personal Data should also be securely destroyed.

### 7. Security, integrity, and confidentiality (Principle 6)

7.1. See Part IV, Section 1 immediately below for more details about Principle 6.

## Part IV: Rights and obligations

### 1. Security

1.1. Principle 6 requires that Personal Data must be Processed securely, and appropriate measures must be taken to protect against unauthorised or unlawful Processing and against all accidental loss, destruction, or damage to the Personal Data.

1.2. Security, integrity, and confidentiality of Personal Data is of paramount importance. CreoPlan Ltd has implemented, and keeps under review, technical and organisational measures and safeguards to ensure the security of Personal Data. Security of Personal Data involves protecting the Personal Data against unauthorised or unlawful Processing and against all accidental loss, destruction, or damage to the Personal Data. CreoPlan Ltd regularly tests the effectiveness of the measures and safeguards it has in place and implements updates where necessary.

1.3. Although measures must be implemented and adhered to in relation to all Personal Data, extra measures and precautions must be considered in order to protect Special Categories of Personal Data and Personal Data that relates to criminal allegations, proceedings, convictions, and offences, given the highly sensitive nature of such data.

### 2. The Data Subject’s rights

2.1. The GDPR provides individuals with lots of rights in relation to their Personal Data. All staff should familiarise themselves with these rights so that they can recognise any requests that may be sent to them by Data Subjects. Those rights include:

a. the right for the Data Subject to have access to their Personal Data (also known as subject access requests, and sometimes incorrectly referred to as 'freedom of information requests');

b. the right for the Data Subject to have inaccurate personal data rectified, or completed if it is incomplete;

c. the right for the Data Subject to have their Personal Data erased (also known as 'the right to be forgotten') (only certain circumstances);

d. the right for the Data Subject to request the restriction or suppression of their Personal Data (only in certain circumstances);

e. the right for the Data Subject to receive or ask for the Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format (only in certain circumstances);

f. the right for the Data Subject to object to Processing of their Personal Data for direct marketing purposes;

g. the right for the Data Subject to object to Processing of their Personal Data (in certain circumstances);

h. the right for the Data Subject to object to decisions based solely on Automated Decision-making, including Profiling;

i. the right for the Data Subject to withdraw their Consent to Processing of Personal Data;

j. the right for the Data Subject to be informed about the Processing of their Personal Data; and

k. the right to complain to the ICO.

2.2. If you receive any of the above requests from a Data Subject, you should immediately contact the **DPO**. The **DPO** will either take responsibility for the request and respond to it accordingly or will advise you what to do.

2.3. It is extremely important that before responding to any request or taking any action in respect of it, that the identity of the person making the request is verified as the Data Subject in order to ensure that Personal Data is not disclosed to any third party or in any way altered or rights exercised by someone other than the Data Subject.

### 3. Disclosure of/sharing Personal Data

3.1. CreoPlan Ltd must only disclose or share Personal Data where it is permitted to do so by Data Protection Laws. As a general rule, this means we must not share or disclose Personal Data to third parties.

3.2. Sharing/disclosing Personal Data can cover many scenarios. In its simplest form, it could be sending Personal Data to a third party by email. However, it can also cover upload (and therefore disclosure) of Personal Data on to systems that CreoPlan Ltd uses but that are run by third parties (e.g. our suppliers and service providers).

3.3. In addition to the above, there are specific rules around the transfer of Personal Data outside of the EEA. The transfer of Personal Data to a country outside of the EEA occurs when that Personal Data is sent or transferred to or viewed or accessed in a country outside of the EEA.

3.4. Where you do need to share or disclose Personal Data to a third party, CreoPlan Ltd must ensure that the following conditions have first been met/are in place:

a. that the third party has a business need to have access to that Personal Data (for example, if they can carry out the services required without the Personal Data or with information that has been anonymised the Personal Data should not be disclosed to them);

b. that the disclosure of the Personal Data was explained in the privacy notice given to the relevant Data Subject; and, if their Consent is required, this has been obtained;

c. the third party has entered into a contract with CreoPlan Ltd that contains GDPR-compliant clauses in relation to the sharing/disclosure of Personal Data;

d. to the extent not covered in a written contract with the third party, CreoPlan Ltd must have received assurances from the third party surrounding the security measures it has in place to protect the Personal Data shared with/disclosed to it; and

e. where the sharing/disclosure will result in a transfer of Personal Data outside of the EEA, that this complies with such safeguards and measures as are required by GDPR.

3.5. If you have any questions relating to the sharing or disclosure of Personal Data, including whether the sharing/disclosure complies with the above requirements, please contact the **DPO** . Before disclosing Personal Data to a new third party or entering into a contract with a new supplier/service provider that involves the disclosure of Personal Data, contact the **DPO**. They can then assist with ensuring compliance with Data Protection Laws and can ensure that all internal policies, procedures, documents, and records are updated (where required).

## Part V: Personal Data breaches

1. A personal data breach is where a breach of security occurs that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

2. Although it is impossible to provide an exhaustive list of what constitutes a personal data breach, examples include:

a. an email containing Personal Data being sent to the wrong person;

b. papers or records containing Personal Data being stolen or left in a public place;

c. access to Personal Data by an unauthorised staff member or by a third party;

d. access to our systems by a hacker or similar authorised access;

3. A personal data breach can be accidental or deliberate.

4. If you become aware of a personal data breach, or if you suspect a personal data breach has occurred or is occurring, you must immediately inform the **DPO** as a matter of urgency. This is especially important because CreoPlan Ltd has limited timescales to investigate the personal data breach and, if required, to report it to the ICO. If you have any records, information, or documentation relating to the personal data breach, you should also provide these to the **DPO** .

5. The **DPO** will be responsible for investigating and dealing with the personal data breach. The **DPO** will decide whether the personal data breach needs to be reported to the ICO and/or relevant Data Subjects. If the **DPO** decides that the personal data breach needs to be reported to the ICO, they will do so within 72 hours after CreoPlan Ltd became aware of the breach.

6. The **DPO** will maintain a register of all data protection breaches (whether or not such breaches are reported to the ICO).

## Part VI: Data-protection-related matters

### 1. Data protection by design and default

1.1. Data Protection Laws require CreoPlan Ltd to ensure that data protection is integrated into all our Processing activities and practices.

1.2. This means that CreoPlan Ltd must implement technical and organisational measures at the very beginning of a project and throughout its lifecycle of its Processing activities, systems, programs and practices. For example, data protection should be at the heart of any new IT systems, services, practices, or policies that involve Personal Data.

1.3. It also means that CreoPlan Ltd must have a data-protection-first approach, such as ensuring that Personal Data is automatically protected by our systems, that only those staff with a business need-to-know have access to the Personal Data, and by ensuring that we only Process Personal Data that is necessary to the purposes for which it is Processed. It is linked to Principle 2 (Purpose limitation) and Principle 3 (Data minimisation).

### 2. Data protection impact assessments

2.1. CreoPlan Ltd must carry out a data protection impact assessment (**DPIA**) for any Processing that is likely to result in a high risk to Data Subjects. A DPIA must also be carried out for:

a. any Automated Decision-making (including Profiling) with legal or similar effects (see this Part, Section 3);

b. large-scale Processing of Special Categories of Personal Data or data relating to criminal convictions or offences;

c. large-scale systematic monitoring of publicly accessible places;

d. use of new technologies;

e. use of Profiling or Special Categories of Personal Data to decide on access to services;

f. large-scale Profiling of Data Subjects;

g. Processing of any biometric or genetic data;

h. matching or combining datasets from different sources;

i. collecting Personal Data from someone other than the Data Subject without providing the Data Subject with a privacy notice;

j. tracking the Data Subject's location or behaviour;

k. carrying out Profiling on children or targeting marketing or online services to them; or

l. Processing any Personal Data that might endanger the Data Subject’s physical health or safety in the event of a personal data breach.

2.2. It is also good practice for DPIAs to be carried out for any major projects that involve the Processing of Personal Data or where Processing is large scale, involves Profiling or monitoring, involves Special Categories of Personal Data, or relates to vulnerable individuals.

2.3. If you think that a DPIA is required, or if you are not sure if one is required, you should contact the **DPO** who will be able to assist you.

2.4. A DPIA must:

a. describe the nature, scope, context, and purposes of Processing;

b. assess necessity, proportionality, and compliance measures;

c. identify and assess the risks to Data Subjects; and

d. identify any additional measures that may reduce those risks.

### 3. Automated Decision-making and Profiling

3.1. Under Data Protection Laws, Automated Decision-making (including Profiling) that has a legal or similar effect on the Data Subject is prohibited unless CreoPlan Ltd meets one of three specific grounds that lifts the restriction.

3.2. Examples of Automated Decision-making include an online decision to make a loan or a recruitment test that uses algorithms and other criteria, and it must be solely automated with no human involvement in the decision.

3.3. Before undertaking any Automated Decision-making, including Profiling, you must contact the **DPO** who will be able to assist you in ensuring compliance with the Data Protection Laws.

3.4. If CreoPlan Ltd carries out Automated Decision-making that does not produce legal or similar effects, it is not prohibited from doing this. However, we must still comply with the Data Protection Laws.

3.5. CreoPlan Ltd must carry out a DPIA if it intends to use Automated Decision-making that produces a legal or similar effect on the Data Subject, but it is good practice to carry out a DPIA for any Automated Decision-making, even if it does not produce legal or similar effects.

## 4. Direct marketing

4.1. Any marketing to customers and other business contacts must be carried out strictly in compliance with Data Protection Laws and laws relating to marketing.

4.2. The marketing laws are complex and depend on how the marketing is to be conducted (e.g. letter, telephone, or email) and who the intended recipients are (e.g. individuals (including sole traders and partners of partnerships) or companies).

4.3. Before undertaking any direct marketing, you must contact the **DPO** who will be able to assist you in ensuring compliance with the marketing laws and the Data Protection Laws.

4.4. Data Subjects have the right to opt out of receiving direct marketing at any time. If you receive a request objecting to direct marketing or a Data Subject opts out/unsubscribes from receiving it, you should promptly ensure that this is noted on our database. Under Data Protection Laws, rather than deleting their details from our database, we are allowed to retain just enough information to record their marketing preferences so we can ensure that no further marketing is sent to them in the future.

If you have any questions about this data protection policy or other matters relating to data protection, please contact the **DPO** using the contact details set out in this policy (Part II, Section 1.3).