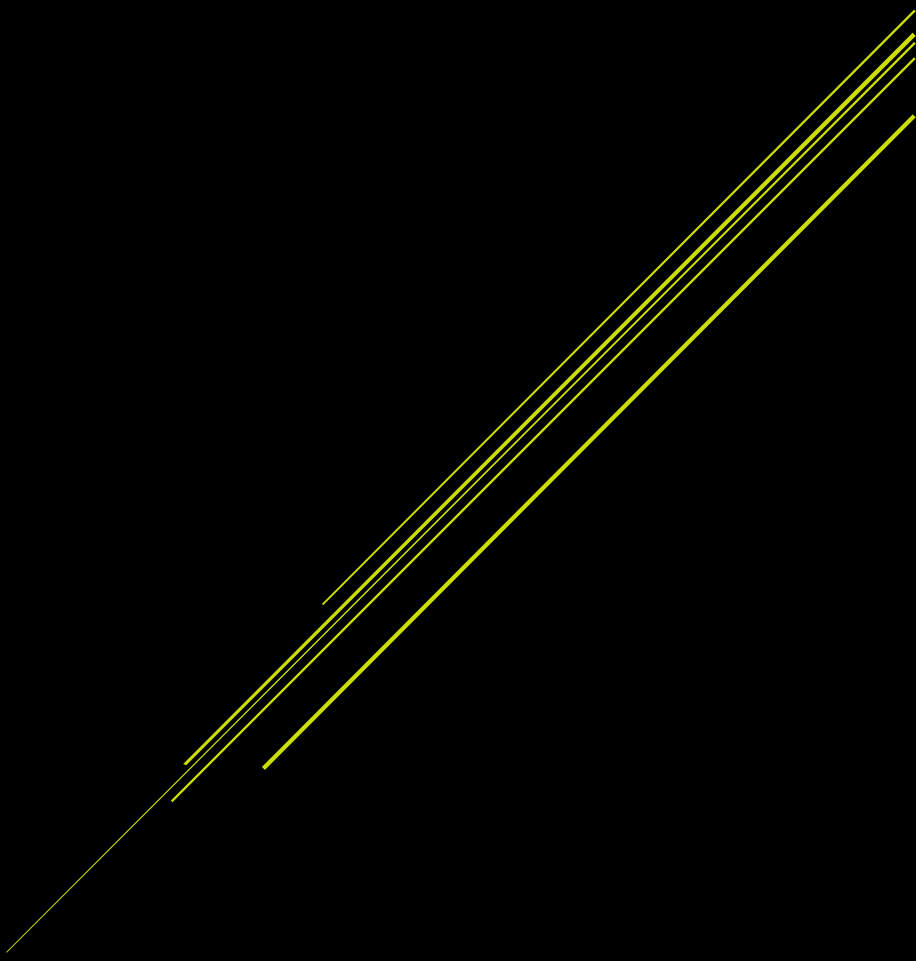

DATA PROTECTION POLICY STATEMENT 2021

4Sight Communications Limited

INTRODUCTION

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. This policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business Purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: • Compliance with our legal, regulatory and corporate governance obligations and good practice • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • Ensuring business policies are adhered to (such as policies covering email and internet use) • Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking. • Service Delivery relating to the products, solutions and services we provide our clients. This data may also be made available to other relevant parties for the purpose of technical support. • Investigating complaints • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments • Monitoring staff conduct, disciplinary matters • Marketing our business • Improving our services
Personal Data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and *CV.*
Sensitive Personal Data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

SCOPE

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

WHO IS RESPONSIBLE FOR THIS POLICY?

As our Data Protection Officer, Simon Turner has overall responsibility for the day-to-day implementation of this policy. Sturner@4sightcomms.com

OUR PROCEDURES

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officer's responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy.
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them.
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.

Responsibilities of the IT Manager

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third-party services, such as cloud services the company is considering using to store or process data.

Responsibilities of the Marketing Manager

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

The processing of all data must be:

- Necessary to deliver our services.
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees.
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers.
- Provides that customers have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, Simon Turner.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Details of third-party organisations used by 4Sight and security specifics for the organisation are held internally, in a document called “4Sight Data storage and security log”, and are updated annually.

Email

Email is an essential and widely used method of communication and information sharing. The scope for a breach or error is very high, as the ability to access data in this format is spread across a wide variety of devices. It is therefore essential that all staff remain highly vigilant and follow the following steps;

- Restrict recipients to those that NEED TO KNOW.
- Check and double check the recipient details before sending.
- Only send relevant information to the relevant people. DO NOT blanket send information.
- Make sure that your devises are adequately protected and secure.
- If you lose your device you MUST IMMEDIATELY inform the DPO. We do have some capabilities to remotely wipe some devices and restrict others.
- If you become aware that a breach of your emails has occurred, or you have distributed information to unintended recipients you MUST IMMEDIATELY inform the DPO.
- Be vigilant about unsolicited email with attachments. Do not open attachments that are remotely suspicious.

- If you accidentally open something and are suspicious that it may have compromised your email, PC or 4Sight systems you must inform your manager immediately.
- Manage your email inbox and sent items and only retain what is relevant and required.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be minimised and where essential must be locked away securely when they are not being used.
- The DPO must approve any cloud used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the company's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones unless required by our contract to service. But even then, this must only be retained as long as is essential.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Data Protection Officer.

SUBJECT ACCESS REQUESTS

Please note that under the Data Protection Act 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests.

Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed, or the contact data has been obtained through a legitimate, compliant source.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar and external approved web based training modules.

It will cover:

- The law relating to data protection.
- Our data protection and related policies, best practice, and procedures.

Completion of training is compulsory for all data controllers.

GDPR PROVISIONS

Where not specified previously in this policy, the following provisions are in effect.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	
Who is collecting it?	HR, Marketing, Operations
How is it collected?	HR Forms, Direct Request, GDPR Compliant Data Sources, Online and Email Requests for contact / Information
Why is it being collected?	Contact required for us to meet or contractual obligations + promote our business.
How will it be used?	Service provision and direct marketing
Who will it be shared with?	Whilst the data is mainly for our own use in the provision of our services we may from time to time need to share data with partner organisations in order to meet with our contractual obligations.
Who are our data controllers?	Head of IT, Head of Marketing, Head of Solutions and Finance Manager.
Details of transfers to third country and safeguards	No transfer requirements are anticipated and therefore prohibited without the consent of the DPO
Retention period	Not more than 12 months when inactive

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing and will have completed an accredited GDPR education course.

Justification for personal data

We will process personal data in compliance with all eight data protection principles. We will document the additional justification for the processing of sensitive data.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden, and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.

Please report all actual or suspected breaches immediately to Simon Turner or Kevin Russell so we can take the relevant measures.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

GDPR AND BREXIT

What is the UK data protection law now the Brexit transition period has ended?

The Data Protection Act 2018 (DPA 2018) continues to apply. The provisions of the EU GDPR were incorporated directly into UK law at the end of the transition period. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK-only context.

On 19 February 2021 the European Commission published its draft decisions on the UK's adequacy under the EU's General Data Protection Regulation (EU GDPR) and Law Enforcement Directive (LED). In both cases, the European Commission has found the UK to be adequate. The draft decisions will now be considered by the European Data Protection Board (EDPB) and a committee of the 27 EU Member Governments. If the committee approves the draft decisions, then the European Commission can formally adopt them as legal adequacy decisions.

Guidance from UK Government:

https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation

Help from the ICO on international data transfers:

https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/international-data-transfers/

The following link to the ICO website includes a checklist on how to assess if data can be transferred internationally:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

European Commission information on data protection following Brexit:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_en

NOTES:

On 19 February 2021, the Commission launched the procedure for the adoption of two adequacy decisions for transfers of personal data to the United Kingdom, under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) respectively.

EU statement regarding EU-US Privacy shield.

The U.S. Department of Commerce and the European Commission have initiated discussions to evaluate the potential for an enhanced EU-U.S. Privacy Shield framework to comply with the 16 July judgement of the Court of Justice of the European Union in the Schrems II case.

CONSEQUENCES OF FAILING TO COMPLY

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact 4Sight Communications Limited DPO sturner@4sightcomms.com