Business security FAQs

PROCESSES, POLICIES & PROCEDURES

Does Vision have a dedicated individual(s) responsible for data protection and/or information security?
Yes. There are several individuals in our organisation that are responsible for security. The principal members of the team are our Data Protection Officer, IS Team, Development Team and Chief Information Officer (CIO). Our Technical team manage our internal security and system security.

Does your organisation have privacy/ data protection /information security policies in force?
Due to the high level of security throughout our company, we hold the ISO27001:2013 certification.

How often does your organisation review and update any policies and procedures?
To ensure that our documentation and processes reflect any changes that may occur, we review and update our policies and procedures frequently. This review occurs annually at the very least and annual continuous assessment visits from our auditors ensure compliance.

Is there a register of subject access requests?
Yes. These requests are managed per department and registered with our HR department.

Do you have a well-defined staff leaver's process in place to ensure that all access to the terminated employee is revoked?
Yes. A leavers' ticket and email is raised by our HR team to our IS team in a timely manner in order to ensure all access is revoked no later than the termination date.

Should someone like to exercise their right of erasure, how soon will this request be carried out? Can you delete or amend any personal data on request and what is your timeframe?
The turnaround for a deletion or amendment can be achieved within 30 days assuming there are no legal reasons to retain the data.

How soon is customer data removed from your system(s) following the termination of service?
This timeframe is dependent on the customer's contract, however, we are able to achieve a termination on our system(s) in line with the contract.

TRAINING AND SECURITY

Do you have any security accreditation in place?
Yes. Vision is ISO 27001:2013

Do you have a secure network architecture in place?
Yes, the architecture of our data centre network is securely provisioned and administered with controlled ingress and egress points. Our external connectivity is also encrypted.

Do you have a clear desk policy that protects against unauthorised access, loss or disclosure arising from data stored on USB devices or printed media?
Yes, we do as this is part of the ISO27001:2013 standard principles.

Is there an acceptable usage policy that states that all personnel are required to understand and comply with their responsibilities regarding the acceptable use of the organisations messaging systems (including email and instant messaging), internet and telephone facilities, which are provided for business purposes?
Yes. Employees are required to take regular ISO awareness briefings class. We also enforce that this class is taken on a new employee's day of induction.

What data protection and/or information security training is provided within your organisation?
All new employees receive ISO 27001 compliant data and security training when joining our organisation. These sessions are conducted by HR, the Internal Systems team and the Data Protection Officer and comprise of system access and data security protocols."

How do you ensure that the equipment and systems used to provide a service are not accessed by the unauthorised users?
We have a security access process in place that assigns rights based on need and to approved users - Role Based Access Control (RBAC)

Does Vision maintain a register of data breaches?
In order to accurately log events that have occurred, we always keep a register of any data breach, no matter the scale. To date, we are able to say that we have not been breached.

How would Vision know whether it had been the object of a data breach?
We have intuitive alerts that are activated via our firewall software, Sophos. Once an alert is triggered, these alerts are sent to our technical team, irrespective of where they are and managed promptly. With this in place, we are sure to adhere to the 72 hours deadline set GDPR to notify customers and the Information Commissioner's Office (ICO) about a possible breach.

In what timescale are data breaches reported to customers?
Vision endeavour to report any breach of a customer's data within 4 hours of awareness and subsequent investigations.

Do Vision perform security/penetration testing and how often do they occur?
PEN testing is completed for all new services and as required for any major changes.

Are technical measures taken to restrict access to systems that hold personal, confidential or sensitive data?
We ensure that all of our personnel have password-protected access to our systems and depending on the type of data and the system, the access is controlled further to only allow a small percentage of staff access and in some cases for a limited period of time. In addition, we also enforce strong password complexity and implement an account lockout mechanisms.

How do Vision enforce security policies and who is responsible for ensuring that these security policies are adhered to?

Our Data Protection Officer and Technical Director oversee all of our security policies.

What security software do you use?
We understand that with security you can never be too careful and due to this, we have achieved our ISO 27001 accreditation because we have taken several measures to ensure that our security and the security of our customers is protected to the highest of standards. To attain this we use the following software: ECSC NCCGroup SecureTest"

How often is access to written or printed material and access to computer systems reviewed?
Access to our systems is reviewed, in some cases, daily. In a majority of instances, it is reviewed monthly in compliance with the ISO27001."

What is your organisations process for the disposal of computer equipment used in processing data?
Any printed personal customer data is securely shredded or placed in confidential waste bins. Any electrical equipment is returned to our IT department for a secure wipe and/or secure disposal.

After a security advisory has been issued, how soon do Vision offer a patch release?
We schedule patch releases every 6 months once they have been tested and compatibility has been assured via our User Acceptance Testing (UAT) system. If a security advisory has been issued, we would accelerate a patch release in line with the supplier's advice."

Who conducts your security audits and what is covered in your security audits?
Vision are audited by BSI annually for continued ISO27001 certification. Internal audits also occur throughout the year.

SUB-PROCESSING

Does Vision outsource, at any stage and to any extent, any personal data processing?
We outsource, to a trusted and audited offshore partner in India, some of the development investigation work however all customer data remains on the UK Vision infrastructure.

Does Vision use a standard data protection contractual clauses in your relationship with third party service providers and third-party data controllers?
Yes. We have a legally binding Non Disclosure Agreement (NDA).
Do you maintain a register of third party data processors to whom you transfer personal data? We seldom transfer any data to any third party. Should we do this, we will always keep a log of the company, date, time and any additional key information as a reference. We also request approval from authorised personnel, usually a CFO or CTO in the form of a signed company letter indicating who has access, what access should be granted and for how long access is required.

What provisions are in place to ensure integrity and confidentiality of any subcontractors/consultants you hire?
In the case that a contractor is required, we would ensure that a signed contractual agreement is in place. This is all in compliance with Vision's ISO27001 protocol.