Data Protection Policy

Byron Business Solutions
Data Protection Policy

As a business Byron is naturally subject to data protection and GDPR regulations and has well established protocols for the protection of information and data stored. In fact, we even train others in this subject.

Mobile devices such as laptops and smart phones are security protected by password and/or face recognition and typically data is securely stored by one of the global respected data storage providers with secure links.

Sensitive data is generally not required by Byron so the risks to individuals are low. Personal information does not usually form part of any training and is therefore neither asked for nor processed or stored.

Data shared between Byron and trainers or clients is generally done using login account and password protected shared documents using secure platforms. To date there has been no breach of this security.

Computers are protected by commercial versions of both anti-virus and anti-spyware and regular scans are carried out to remove any suspicious files which may have been installed via the internet.

All staff are fully aware of the risk of viruses, trojans, worms or other methods of infection and report any suspicious for further investigation.

No complaint, claim or allegation has been received from a client in connection with any loss of or inappropriate use of any data. Trainers are bound contractually to respect all data and severe sanctions would be used should this be breached.

We take a common sense approach and we risk manage all activities.