TOUCHRIGHT SOFTWARE - GDPR INFORMATION

Where are your data and applications stored?
All data is stored and hosted on our Amazon Web Services server.

Is that data ever moved out of the European Economic Area (EEA)?
No all data is stored on servers located in Ireland.

Do you ever transfer data between data centres outside of the EU?
No.

Do you always inform me when my data is being transferred?
We do not transfer data.

Do you have a Data Protection Officer?
Yes - Rachel Lightfoot, Director.

What data controls and risk management processes do you have in place?
Our systems are secure and can only be accessed with a password, which is encrypted. It's in your interest to make sure that your passwords are secure and you can change your password at any time by logging into the dashboard and going to My Account/User Profile. We store an encrypted version of each password which we can use for authenticating a user but we cannot see the plain text version for security purposes. All data that is sent from or to the TouchRight app and dashboard is transmitted securely using HTTPS protocols. We are also implementing data breach protocols on our AWS server which will be in place by 25th May 2018.

How do you manage the version release process on your platform to ensure adequate level of data protection?
TouchRight controls its own AWS access keys and determines who is authorized to access their AWS account. AWS does not have visibility of access keys, or who is and who is not authorized to log into an account.

TouchRight monitors and controls use, misuse, distribution or loss of access keys.

Who can access my data, under what circumstances, and what can they see? Is this access tracked?
All of your users have access to your data, and users with Account Owner permissions can control which users are able to access your account and data and have permission to disable or delete users at any time.

TouchRight internal staff have access to customer accounts to deal with support queries, plus we use a number of third party subcontractors to assist with the provision of it service. Our subcontractors have access to customers' content, but only where it is required to assist with technical and support issues. TouchRight only uses subcontractors that we trust and we use appropriate contractual safeguards which we monitor to ensure the required standards are maintained.

TouchRight only uses your staff/internal user details for product/software updates only, and never for marketing purposes. TouchRight does not sell, distribute or lease your internal or external personal information to third parties for any purpose, including marketing.

Can I audit your security and technical measures on the protection of data?
Dependent on the level of systems access required, yes this could be organised if required.

Do you have a security breach notification process in place?
Yes. In the event that a data breach does occur and is likely to result in adversely affecting individuals' rights and freedoms, we will inform any affected customers immediately and notify the ICO of the data breach within 72 hours of becoming aware of it. We will also keep a record of any personal data breaches, regardless of whether we are required to notify.

Do you currently adhere to Binding Corporate Rules (BCR)?
No.

Do you have measures in place to become GDPR compliant in time for May 2018?
Yes.