Digital Log Book & GDPR

Digital Log Book & GDPR

Digital Log Book (DLB) has GDPR compliance central to everything we do.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

Some GDPR Key Points

1. Explicit permission. When you give permission to an app or website to have or use your details in a specific way, they cannot use it for any other purpose or, crucially, sell it on to third parties.
2. Clear and affirmative consent will be needed before private data is processed and this will require an "active step" such as ticking a box. GDPR is clear that "silence, pre-ticked boxes or inactivity will thus not constitute consent. In future, it should also be as easy for a person to withdraw consent as to give it."
3. Data portability gives you the right to ask for any data that a company has about you, which should be returned in a machine-readable format, so that you can reuse it, for example to give it to another service provider. The Digital Log Book is yours to keep wherever you move to, it belongs to you and your data stays with you.
4. Clear limits on the use of profiling. There are new limits where automated processing of personal data is used to "analyse or predict a person's performance at work, economic situation, location, health, preferences, reliability or behaviour", including credit worthiness. Under the new regulation, profiling would generally only be allowed with the consent of the person concerned, where permitted by law or when needed to pursue a contract and should comprise a human element, including an expectation of the decision to be reached.
5. Privacy by design means that when you download an app or sign up for a service, you should not be asked for data that is not directly needed or relevant for the purposes of interacting with that app or service.
6. Giving someone access to your data does not mean they will always have access to it. You control who has access to your data from when you shared it to when you cut their access off. Under the GDPR you have a right to be forgotten and will be able to ask companies or platforms to delete your data if you no longer want them to have it. The two caveats to this are;

    a) that this will not apply to some information that there is a legal requirement to keep, for example medical records, and;

    b) that it is also a personal right to forget, distinct from the 3rd party Right to be Forgotten, where individuals can request that outdated or undesirable information about them be removed from search engines.
7. The new rules promote techniques such as anonymisation (removing personally identifiable information where it is not needed), pseudonymisation (replacing personally identifiable material with artificial identifiers), and encryption (encoding messages so only those authorised can read it) to protect personal data.

Further information can be found at the ICO - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr