Jabra GN

Jabra Xpress & Jabra Direct

Engineered to be secure

Why is data security important?

- Level of cybercrime is increasing.
- News stories on data leaks are becoming more common.
- New requirements from governments relating to GDPR.

How do Jabra protect data?

- With Jabra Xpress/Direct data is collected and managed by Jabra in a secure way. First and foremost, only the necessary data is collected. This is protected using best industry practice.
- Jabra uses the internationally recognized standard, SOCII (latest version), as a framework for the declaration of confidentiality and security, showing that we minimize security risks where possible.
- Jabra Xpress/Direct and the processes used around these products are audited by a 3rd party – one of the 'Big 4' consultancy companies – to secure that the solution lives up to the requirements.

Key areas of the SOC II program include implementation of several security principles, such as identification and mitigation of security risks.

What does this mean in practice?

- Security is integral to the design of the Jabra Xpress & Jabra Direct solution.
- Access is restricted by user-id and password, and passwords must meet certain requirements.
- Data is kept secure both at rest and in transit.
- Users of Xpress/Direct cannot see each other's data.
- The solution is compliant with GDPR.
- Data is anonymized, so in the unlikely event of a leak, data cannot be traced back to the source, making the likelihood of data being misused very small.
- In case of incident, a dedicated process and department are in place to act.

Should there be any further questions, these can be directed to your commercial contact person, or alternatively forwarded to security@jabra.com.