The General Data Protection Regulation (GDPR) – Activetrail

The following are answers to frequently asked questions by ActiveTrail customers from the EU and worldwide regarding our compliance to GDPR.

In general, ActiveTrail is compliant with GDPR and has gone to great lengths in order to protect, document and revise processes relating to its customer's data security and privacy.

Records of Processing Activity and Data Inventory

Q: Has ActiveTrail documented its data processing activities and data Inventory?

Yes. Activetrail has documented of all of its Records of Processing Activity (ROPA) and Personal Data Inventory (PDI) which have been reviewed by an international third party. As part of Activetrail's GDPR preparation, Activetrail reviewed all of the internal processes and procedures and documented them as required by regulation.

DPO

Q: Has ActiveTrail appointed a DPO?

Yes. ActiveTrail has a DPO which is responsible for all of the data protection issues (including, but not limited to, GDPR).

CISO

Q: Does ActiveTrail have an appointed Security Officer?

Yes. ActiveTrail has a Chief Information Security Officer (CISO). Security is our top priority at ActiveTrail, and as part of our ongoing efforts, among many other precautions and investments in software, procedures, knowledge and human resources, ActiveTrail is in process of receiving its ISO 27001 security certification.

Data Protection and Record-keeping Policy

Q: What is ActiveTrail's record-keeping policy?

Activetrail keeps all account data indefinitely, as long as the user is active. If a user closes its account, and after a period of 24 months, all account data is deleted (except for legal and financial data, which we are obligated to keep). If an ActiveTrail customer actively requests to be deleted, we will handle the request within 48 hours (except for legal and financial data, which we are obligated to keep).

Data access

Q: What is ActiveTrail's policy regarding access of data?

Activetrail has Role Based Access Controls (RBAC) in place. All Access to data is restricted to limited personnel and requires several security authorizations and layers.

Internal confidentiality and data usage

Q: How does ActiveTrail treat its customers data confidentiality and usage?

ActiveTrail's customer accounts store private data that belongs exclusively to the customer. ActiveTrail does not share or manipulate any data between accounts and does not make any use of any data stored or processed in a customer's account. All accounts are segregated and access is protected by ActiveTrail's password protection policy requiring, among other things, password change every 90 days, strong passwords etc. In addition, Activetrail uses some third party software for analytics, monitoring, security etc. but no personal data is shared with any third parties.

IT security policy

Q: What is ActiveTrail's IT security policy?

ActiveTrail maintains a very high level of security and is in process of receiving its ISO 27001 security certification. Among other things, ActiveTrail runs anti-virus and anti-malware software on all its stations and servers, a DLP system, and a prevention, detection and response system on all of its technology including a 24/7 security human response team. ActiveTrail's hosting facility is in the EU and is a private server farm within a highly secured facility with the following standards: ISO 14001:2004 | ISO 22301:2012 | ISO 50001:2011 | ISO 9001:2008 | ISO/IEC 27001:2013 | OHSAS 18001:2007.

anonymization of the data

Q: Which data does ActiveTrail Anonymize?

Activetrail encrypts all usernames and passwords. All other data is not anonymized and is deleted as explained above. ActiveTrail recommends that customers do not store user sensitive data such as financial or medical information since this is not the primary use of the platform.