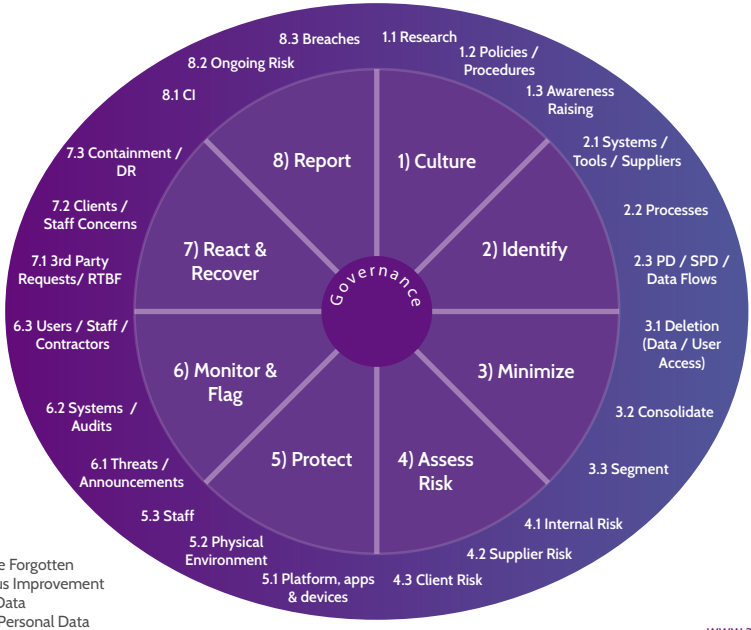
An Overview of our GDPR Policy

agileChilli GDPR Action and Continuous Improvement Plan v16



Key

FTBF	Right to be Forgotten
CI	Continuous Improvement
PD	Personal Data
SPD	Sensitive Personal Data
DR	Disaster Recovery

www.agilechilli.com

As of May 2018 the EU's new GDPR came into effect and SaaS organisations such as ourselves are responsible for both the security and privacy of the data held on our own systems and the systems we provide our clients.

The model above, based around 8 core themes, offers a high level overview of these responsibilities.

As of May 2018 the EU's new GDPR came into effect and SaaS organisations such as ourselves are responsible for both the security and privacy of the data held on our own systems and the systems we provide our clients. The model above, based around 8 core themes, offers a high level overview of these responsibilities.

Article 24 of GDPR:
The controller shall implement appropriate
a) technical and b) organisational measures
to ensure and to be **able to demonstrate** that
c) processing is performed in accordance with this Reg.
d) those measures shall be reviewed and updated where necessary.

Overview

Step 1) Culture: As a SaaS provider we need to educate both ourselves and our clients about the impact of this regulation on our respective businesses to allow us to build a genuine culture of compliance.

Step 2) Identify: We then need to create a comprehensive register of where data processing takes place, what data is being held because of this processing and how it flows from our systems to other 3rd party ones.

Step 3) Minimize: We need to delete any old high risk or low value data, and user accounts that are no longer of any real use. Also we should consider moving personal data from difficult to monitor tools, (e.g. spreadsheets) to more secure systems.

Step 4) Assess: We then need to assess the risk associated with processing the remaining data in the identified systems.

Once we know our risk exposure we can decide how best to manage that risk.

Step 5) Protect: We then need to work how we might best protect the data we retain, and prioritise our efforts to get the best return on our investment of time and money (e.g focus first on high risk personal data).

Step 6) Monitor & Flag: We also need to put in place systems to monitor any activity that might require investigation and have in place policies to rapidly address flagged concerns etc.

Having done our best to reduce any BAU risk we now need to plan how to handle any failure.

Step 7) React & Recover: We need to be ready to respond to both day to day queries about the data we retain from various stakeholders within the time guidelines laid down within the regulations and to any breakdown in our data security measures.

Step 8) Report: We also need to have procedures in place to report not only breaches failures but also an unusual activity, to the relevant authorities and customers.

Step 9) Track Progress: Finally we need to track how quickly we are progressing towards our goals.

Further Information

If you would like a more detailed understanding of our current state with regard to GDPR compliance please contact Clifford Calcutt on 0117 3210104 or email us at datasecurity@agilechilli.com and ask for the up to date version of our full GDPR / Continuous Improvement Review document.