GDPR Compliance Service

May 25th, 2018 marked the enforcement of the most comprehensive privacy / data protection law in the history of the EU. Despite its predecessor (the Data Protection Directive) having been enforced into national laws for the previous 20+ years (e.g. the Data Protection Act in the UK became law in 1998), the majority of organisations still had little idea where to begin.

The General Data Protection Regulation (GDPR) is not the easiest read. Written by lawyers, the language often seems ambiguous with significant room for interpretation. While CCS in no way considers itself an expert in privacy and data protection law, every GDPR compliance project must begin exactly the same way; with your data.

The CCS GDPR Compliance Service will provide you everything you need to get to the lawful basis for processing[1]:

1. A comprehensive data asset inventory with recommendations for anonymisation, pseudonymisation, minimise retention, or outright deletion;
2. A mapping of all personal data flows against business processes;
3. A mapping of all data assets to internal, international, and/or outsourced data repositories;
4. A list of all relevant 'upstream' and 'downstream' third parties;
5. A breakdown of security controls per repository

Given the above information, most data protraction experts can make the determination of lawful basis, then provide all necessary documentation to make the organisation 'compliant'.

Depending on your circumstances, this may include:

1. Develop a complete set of appropriate data protection policies and standards to adequately demonstrate accountability (Art. 5(2));
2. Legalise data transfers between legal entities under the *same* corporate umbrella with some form of "*legally binding and enforceable instrument*" e.g. an Intra-Company Data Transfer Agreement (ICDTA) using "*standard data protection clauses*".
3. Data Processing Agreement(s) (DPA) for relevant third parties;
4. Assurance that contracts in place with third party data sources include guarantees that the data was collected fairly and lawfully;
5. Legalise data transfers to third countries outside of an 'adequacy' decision with a Data Transfer Agreement (DTA), binding corporate rules, a Code of Conduct, and/or certification (when it becomes available);

[1] Determination of the lawful basis for processing can be handed off to CCS legal partners.

6. Performance of Legitimate Interest Assessment(s) (LIA) to ensure that the organisation's interests are appropriately "*balanced against the individual's interests, rights and freedoms*";
7. Performance a Data Protection Impact Assessment (DPIA) if necessary;
8. Account for variances in national laws (if applicable);
9. Submit record of processing activity to a supervisory authority (per Article 30)

Methodology

CCS utilises a proven methodology, developed of the course of multiple engagements, to help organisations achieve *sustainable* compliance.

CCS uses one or preferably both of the following methods:

1. *Manual, interview-based questionnaires and guidance*: CCS will conduct a series of expert-led sessions with subject matter experts from each department or line of business; and / or
2. *Automated, Data Loss Prevention (DLP) powered data discovery*: CCS will utilise industry leading DLP solution to discover and map the flows of structured and unstructured personal data throughout the environment.

Neither solution is perfect, the best results are only obtained when the above options are used in concert.

That said, the manual solution will prove adequate in most situations as compliance with GDPR is achieved with best efforts, not perfection. Lawyers will call this 'reasonable', or 'appropriate' as longs as the effort and output matches 'precedent'.

Assessment Plan

A more detailed Project Definition Plan (PDP) will be made available well in advance of project kick-off, but in essence:

Phase 1: Kick-Off / Program Goal Confirmation (performed on-site)

- Meet with senior leadership to reinforce commitment and agree the overarching *business* goals for the GDPR compliance program;
- Meet with key stakeholders to agree project activities;
- Meet individually with key stakeholders to discuss department / LoB specifics with regard priorities and resource availability;
- Agree all next steps, timelines, and functional responsibilities;

Phase 2: Project Plan Definition (performed off-site) - *Optional*

- Work with client project manager to produce comprehensive project plan.[2]

Phase 3: Program Execution (performed on and off-site)

[2] CCS does not provide a project management function, but will work with whomever client assigns (if applicable).

- Details vary significantly per unique business, but this Phase encompasses the execution of work across all departments / LoB.

Phase 4: Project Close (performed on-site)

- The CCS GDPR Compliance Service can be seen as a stand-alone service, or as an eventual stepping-stone towards full certification. Whatever the goals of the organisation, the project close is designed to hand-over all remaining action items to designated owners.

Timeframe

The process for executing a GDPR compliance program can only ever be unique to each organisation, and depending on available resources/skill-sets/budget, the consulting time required will vary enormously.

In the end the timeframe will depend entirely on the organisation in question, CCS is there to support the work performed and guide stakeholders towards their agreed deliverables.

Deliverables

- A comprehensive data asset inventory with recommendations for anonymisation, pseudonymisation, minimise retention, or outright deletion;
- A mapping of all personal data flows against business processes;
- A mapping of all data assets to internal, international, and/or outsourced data repositories;
- A list of all relevant ‘upstream’ and ‘downstream’ third parties;
- A breakdown of security controls per repository
- Recommended next steps