ANNEX 2 - GDPR Action Plan

Last Updated - 07th Janaury 2018 (MN)

Ref.	Task	Official Guidance Status	Official Guidance	Depends On	Status	Notes
1.0	**Information Asset Register**					
1.1	Identify Information Assets (inc. location, retention, and format).	May 2017 (ICO website)	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/		Complete	RDC to allocate IAOs and provide populated spreadsheet to Veritau. Veritau to then collate and identify areas of work and compliance.
1.2	Identify whether organisation holds information assets as data processor or data controller.				/	RDC to allocate IAOs and provide populated spreadsheet to Veritau. Veritau to then collate and identify areas of work and compliance.
1.3	Identify which job positions should be information asset owners (seniors, managers, senior managers).				Complete	RDC to examine this as part of HR
1.4	Modify job descriptions to include information asset owner as a responsibility.				/	RDC to examine this as part of HR
1.5	Ensure IAOs know their responsibilities as IAO.				Complete	Veritau to deliver training and guidance
1.6	Establish a retention/deletion schedules				/	Veritau to examine existing schedule and identify needs
2.0	**HR**					
2.0	Review employee contracts & identify reliance on consent and alternatives to consent	June 2017 (XpertHR) - Not Official	U:\Personal\Misc\XPert HR - GDPR.p		/	This area to be examined once IAR is established and agreed
2.1	Establish retention periods for HR records.	June 2017 (XpertHR) - Not Official			/	This area to be examined once IAR is established and agreed
2.2	Modify job application forms to ensure compliance with GDPR.	June 2017 (XpertHR) - Not Official			/	This area to be examined once IAR is established and agreed
2.3	Modify reference request forms to ensure compliance with GDPR.	June 2017 (XpertHR) - Not Official			/	This area to be examined once IAR is established and agreed
2.4	Update grievance and disciplinary policies to ensure compliance with GDPR.	June 2017 (XpertHR) - Not Official			/	This area to be examined once IAR is established and agreed
3.0	**Fair Processing and Consent**					
3.1	Review all fair processing notices to ensure compliance with current ICO guidance.	Oct 2016 (ICO)	https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/		/	This area to be examined once IAR is established and agreed
3.2	Identify any processing based on consent and review whether consent is 'freely given' according to ICO guidance.	March 2017 ICO. Consultation only	https://ico.org.uk/about-the-ico/consultations/gdpr-consent-guidance/	WP29 guidance due later 2017	/	This area to be examined once IAR is established and agreed
3.3	Issue FPNs should any processing no longer rely on consent (3.2)	May 2017 (ICO website)	https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/	above	/	This area to be examined once IAR is established and agreed
3.4	Ensure FPNs are visible on public website (unless not appropriate)	May 2017 (ICO website)	https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/	above	/	This area to be examined once IAR is established and agreed
4.0	**Contracts and Service Level Agreements**					
4.1	Review all contracts and agreements with clients to establish who is data processor and data controller .	May 2014 (ICO)	ICO: Data controllers and data processors 2014 05 27	beware further guidance	/	This area to be examined once IAR is established and agreed
4.2	Review all contracts and agreements with clients to ensure compliance with GDPR.				/	This area to be examined once IAR is established and agreed
4.3	Amend all contract templates to reflect GDPR legislation.				/	This area to be examined once IAR is established and agreed
4.4	Review all third party contractor agreements (i.e payroll etc) to establish who is data processor and data controller	May 2014 (ICO)	ICO: Data controllers and data processors 2014 05 27	beware further guidance	/	This area to be examined once IAR is established and agreed
4.5	Review all contracts and agreements with all third party contractors to ensure compliance with GDPR.				/	This area to be examined once IAR is established and agreed
4.6	Amend all third party contractor templates to reflect GDPR legislation.				/	This area to be examined once IAR is established and agreed
5.0	**Information Rights**					
5.1	Create or update a policy for the rights of data subjects.	May 2017 (ICO website)	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/		Draft Policy Created	Veritau to create overarching process/policy/FPN to be modified and agreed by RDC
5.2	Amend SAR procedure for shorter period but include possible extension		https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-of-access/		Draft Policy Created	Veritau to create overarching process/policy/FPN to be modified and agreed by RDC
5.3	Devise process for requests for rectification inc follow-through		https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-rectification/		Draft Policy Created	Veritau to create overarching process/policy/FPN to be modified and agreed by RDC
5.4	Devise process for requests for erasure inc refusal		https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-erasure/		Draft Policy Created	Veritau to create overarching process/policy/FPN to be modified and agreed by RDC

ANNEX 2 - GDPR Action Plan

Last Updated - 07th Janaury 2018 (MN)

Ref.	Task	Official Guidance Status	Official Guidance	Depends On	Status	Notes
5.5	Ensure there is a policy and procedure for 'data portability'	January 2017 (A.29 WP)	http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083		n/a	Decided that this is not going to be relevant to RDC so has not been included in Policies. CIGG should review this descision.
6.0	**Training**					
6.1	Choose an appropriate GDPR training package (in house or external)	N/A			Complete	Training sessions for 2018-2019 will be delivered by Veritau withinin allocation of hours
6.2	Create a training schedule to ensure all employees are trained in GDPR before legislation enforcement date	N/A			/	Veritau to deliver IAO training with key messages to pass down to staff RE GDPR (2x2 Hour Sessions) - Once other action points are agreed
6.3	Set a review date when all employees must refresh training.	N/A			/	Veritau to deliver IAO training with key messages to pass down to staff RE GDPR (2x2 Hour Sessions) - Once other action points are agreed
6.4	Ensure GDPR training is mandatory for all new starters and temporary/seconded officers.	N/A			/	Veritau to deliver IAO training with key messages to pass down to staff RE GDPR (2x2 Hour Sessions) - Once other action points are agreed
7.0	**Roles and Responsibilities**					
7.1	Appoint an accountable Data Protection Officer and change job description accordingly.	January 2017 (A.29 WP)	http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083		Complete	RDC Happy to take on Veritau as DPO
7.2	Ensure the SIRO briefed on GDPR implications and sanctions.	May 2017 (ICO) - Draft Only	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/		Ongoing	Ongoing
8.0	**Policies and Procedures**					
8.1	Ensure all policies are compliant with GDPR.	N/A			Draft Policies Created	Need to establish IAR and need more guidance before this task can be completed
8.2	Ensure privacy policy is updated to reflect changes to GDPR.	May 2017 (ICO) - Draft Only	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/		Draft Policies Created	Need to establish IAR and need more guidance before this task can be completed
8.3	Ensure that project framework includes a mandatory data protection impact assessment (DPIA) as part of privacy by design.	May 2017 (ICO) - Draft Only	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/		Ongoing	Need to establish IAR and need more guidance before this task can be completed
8.4	Update publication scheme based on review of information assets (1.1)	N/A			/	Need to establish IAR and need more guidance before this task can be completed
9.0	**Information Security Incidents**					
9.1	Ensure organisation's breach reporting procedures are effective enough to report to ICO within 72 Hours	TBA (A.29 WP)		WP29 guidance due later 2017	Draft Policy Created	Veritau to update/write Information Security Incidents procedure and suggest that Veritau coordinate data breaches for RDC because greater emphasis on reporting to ICO under GDPR.
9.2	Ensure training schedule addresses data security incidents under GDPR	TBA (A.29 WP)		WP29 guidance due later 2017	/	To be delivered as part of IAO training
10.0	**additional controls**					
10.1	Review all 'data matching' and 'profiling' processing that the company does, for itself or on behalf of a client, and ensure the processing if compliant with GDPR	April 2017 (ICO) - Draft Only	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/	WP29 guidance due later 2017	/	Likely to be found in very few services but can be established once IAR is finalised.
10.2	Ensure all relevant staff are trained and understand the risks of data matching and data profiling.	April 2017 (ICO) - Draft Only	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/	WP29 guidance due later 2017	/	To be delivered as part of IAO training - furhter specific training can be delivered if neccesary
10.3	Identify any processing of genetic or biometric data	April 2017 (ICO) - Draft Only	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/	WP29 guidance due later 2017	/	Likely to be found in very few services but can be established once IAR is finalised.
10.4	Identify any data transfers outside EEA	April 2017 (ICO) - Draft Only	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/	WP29 guidance due later 2017	/	Likely to be found in very few services but can be established once IAR is finalised.