General Data Protection Regulation - Readiness Assessment

Category	Recommendation #	Recommendation	Priority	Action Plan Updates	Due	% complete
Data Protection and Privacy Management	R01	Establish a full time information governance working group and nominate Data Protection champions	Medium	Information Governance Group already in place - Nominate DP Champions by Sept 2017 - Training for champions on new regs - early Oct 17	Jan-17	100%
	R02	Establish KPI's to measure Data Protection performance	Medium	Develop a KPI for Data Compliance	Dec-17	Not started
	R03	Decide on how the role of DPO will be filled moving forward and make a suitable appointment, document the process behind the appointment	High	Scope requirements Discuss with SLT Appoint and train (if required) **Update 26/10** - DA appointed, training required	Sep-17	75%
Policy Framework	R04	Review and improve the governance framework to include policies required by GDPR, such as privacy impact assessment etc. Test existing policies against GDPR requirements and amend where necessary. Introduce periodic audit, testing and review of controls Update the document register to include new policies, procedures and work instructions	Medium	- Review and rerefsh DPA Policy for GDPR - Update FOI policy - Update SARS Policies Test policies , spot check etc	Jan-18	25%
Information risk assessment and management	R05	Ensure that data protection or GDPR is placed on the corporate risk register to raise the profile of data protection compliance	Low	Risk added to register	May-17	100%
	R06	Design and maintain an information risk register, ensuring that it is sufficiently granular to accurately record information risks and mitigation. Ensure that it is periodically reviewed	Medium	Information Risk Impact Assessment template developed Communicate to organisationonce Information Asset Owner training undertaken	Nov-17	0%
	R07	Define and implement a policy and procedures on privacy impact assessments (PIA's). Ensure that the PIA processes encompasses the requirement to consult the Regulator in certain circumstances	Medium	- Draft policy and procedures (ICO have guidance) - Training for staff	Jan-18	10%
Training and awareness	R08	Ensure that data protection training continues to be provided on induction and on at least an annual refresher basis. Supplement this with more frequency (monthly) awareness raising of relevant issues or changes in policy. Consider designing or procuring bespoke training for thoe who require greater training than an e-learning module can provide	Medium	Push final people to conclude training and refresh in 12 months time. Need to look at further training for key individuals GDPR specific training package developed - roll out March 2018	ongoing	70%

Audit and compliance checking	R09	Introduce compliance checking and audit processes that comply with GDPR's requirements the scope of which will ensure that evidence will be available to demonstrate that South Hams DC complies with the GDPR. Appoint appropriate Audit team, internal and external. As a guide this is likely to be at least Annual Audits of all data protection policies and operating procedures and the gathering and recording of objective evidence of compliance and /or the raising of corrective action requests to modify behaviour in line with policy	Medium	- Already have an audit team - to be built in to their annual work plan Becomes BAU from that point onwards	Jan-18	0%
Overview and purposes of data processing activities	R10	A register of data processing purposes should be compiled and maintained	High	- Register template developed - training being refined - IAO's to complete register by Jan 2018	Jan-18	25%
Lawfulness of processing	R11	Improve evidence of data processing control by reviewing all data that is held and documenting its purpose and lawful grounds for processing particularly in regard of sensitive personal information and behavioural information. Compile a register of data processing purposes as set out in the recommendation R10 and ensure that the lawful grounds for processing are marked against each data processing purpose.	Medium	This will be covered as part of R10		
	R12	To ensure that South Hams is able to demonstrate control over its data acquisition processes it is necessary to review all sources of personal data, compile a register of data sources, and ensure there is a process for keeping up to date	Medium	Once R10 completed review can take place	Feb-18	0%
Information processing systems, flows and information	R13	Maintain and, if necessary, expand the information asset register			Business as usual	
	R14	Document key data flows to ensure a thorough understanding of how data is captured and moved about the South Hams Data systems			Business as usual	
Nature of data being handled / processed	R15	Create a system to maintain information describing and defining the data being handled by the Councils and the categories of data subject	Low	- Once R10 completed this can be undertaken (majority will be via W2)	Mar-18	0%
	R16	Create a data sharing policy setting out a standard process for employees to follow to lawfully share and/or disclose persona data, including appropriate pre-contract due diligence	Medium	Drafted, needs review Built in to contracts as part of drafting	Mar-18	25%
	R17	Establish a register of data sharing agreements/arrangements and ensure that a geographic review of all data processors is undertaken once a full list is compiled	Medium	- linked to contract database development - CM support required to extract data from contracts into simple spreadsheet	Apr-18	5%

Data sharing and use of data processors	R18	Ensure that an agreement is in place with all instances of outsourced processing and/or sharing. Test each agreement to ensure that a) the terms are in the Councils favour and compliant with the needs of GDPR; b) indemnities are appropriate; and c) the data processing instructions issued are effective. Consider creating standardised templated agreements	Medium	- Legal to undertake review of agreements (although no large scale outsourcing undertaken in SH)	Apr-18	0%
	R19	Undertake a privacy impact assessment on the data processors used in order to properly assess the risks that it might pose and/or to document the measures taken to ensure that adequate protection is in place .	Medium		May-18	0%
Data Transfer Protocols	R20	Review existing transfer arrangements and introduce a policy defining approved secure data transfer and operating procedures for employees. If ecel and email are to be used ensure that spreadsheets are password protected or encrypted			Feb-18	0%
International Transfers	R21	Review all data sharing and transfers to test if data is transerred outside of the UK and test the adequacy of arrangements where international transfers occur	Low	Not aware that we make any international transfers of data	n/a	100%
	R22	Introduce a process for periodically reviewing the aqecuacy arrangement for all overseas processors to ensure that their adequacy arrangement does not lapse and for ensuring that new arrangements are not put in place without appropriate due process	Low	Not aware that we make any international transfers of data	n/a	100%
Data Quality and Accuracy	R23	Draft a data quality policy focusing on how different types of information will be maintained accurately. Give emphasis in particular to data such as communication preferences, volatile data which may change frequently, and data which would cause harm / distress to the subject if it is incorrect	Low	Policy drafted, just needs finalising then adding to policy library	Dec-17	50%
Data Minimisation	R24	Undertake a deep dive review of data being handled by South Hams DC and consider what steps would be appropriate to review and maintain accuracy	Low	- wait until IAO training delivered	Business as usual	0%
Data Retention	R25	Review the data processing purposes and data used for each processing activity and determine how long it needs to be held in a format allowing identification of data subjects for the purpose (s). Review which mechanisms would be appropriate in each of the cases to enable South Hams to comply with the 5th data protection principle	Medium	- Complete information asset register - undertake review / interview with IAO to assess actuall processing purposes	Mar-18	0%
	R26	Carry out a deep dive exercise on data retention across all information assets then review and disseminate the RM policy and retention schedules for compliance and work-ability	Medium	Will be undertaken with any high risk areas identified in R25	Apr-18	0%

IT Management	R27	Review ICT policy framework to ensure that they are aqequate for GDPR purposes	Medium	-policy review underway, new policy tool in place for staff to accept policies	Jan-18	40%
Monitoring and testing control measures	R28	Consider using dedicated log servers to improve logging of events on the systems and also increasing the frequency of IT security audits	Medium	Optional / not required for compliance		0% optional
Distruction and Disposal	R29	Document how redundant equipment and media are to be disposed of	Medium	Confirmed destruction contract in place for redundant equipment and media		100%
Disaster Recovery and Business Continuity	R30	Review existing arrangements and test for GDPR compliance	Medium	- Disaster recover plan being reviewed Oct / November 17 - With ELT for input into timescales	Mar-18	50%
Security events , incidents and breach management	R31	Review incident reporting provisions to ensure alignments with GDPR. Remind employees through awareness and training	Low	place. Reminder to be circulated to all staff about what should be reported and	Feb-18	75%
	R32	Review all processor contracts for information security breach notification provisions	Low	- Lined to completion of contracts database	Feb-18	0%
Right to information and transparency	R33	It is recommended that all privacy statements and privacy forms re correlated and reviewed to ensure compliance with the GDPR. Consider placing website privacy policy in a more prominent location	Medium	- Review existing forms (March 18) - Update and ensure live May 18	May-18	0%
	R34	Introduce work methods to ensure that privacy information and its publishing / deployment are strictly controlled	Medium	- Updates to managers / IAOs in terms of requirements	Mar-18	0%
	R35	Devise a fair processing strategy that provides a workable layered approach to privacy information	Medium	- Drafted Jan 18 (first draft started) - communicated Feb 18 - On website - April 18	Apr-18	0%
	R36	Review data systems to ensure that they are able to record what privacy information each data subject has been provided with	High	- review capability of W2 for this process - review to be taken out by Dec, with solution in place May 18	May-18	0%
Right of access	R37	Amend SAR policy and process to ensure that it is GDPR compliant and ensures employees are trained in its application	Medium	- Under review currently - Training for Team Leaders to be arranged April 18 (GDPR online course includes module)	May-18	25%
Right to object to processing	R38	Establish a mechnism for logging any objection and determining the extent to which the legitimate interests might over-ride those data subjects	Medium	- Talk to other Councils about their approach / advice from ICO - Agree process by March 18 - Training April 18	Mar-18	0%
Right to object to direct marketing	R39	Review current arrangements for recording objects to direct marketing	Low	- Talk to comms to understand how information handled - Agree approach for future	Feb-18	0%

Right not to be subject to automated processing and profiling	R40	Review data processing activities and test them against automated decision making rules	Medium	- Assessment with ICT of any automated decision making processes - If any, review testing results	Apr-18	0%
Right to restriction of data processing	R41	Define and implement a method of applying restricted processing to data where a relevant objection is received	High	- W2 process to be amended for individuals objecting to processing - needs a warning note	Feb-18	0%
Right to correction / erasure of data	R42	South Hams should review its processes for executing R2BF requests and also improve its understanding of who data is shared with or disclosed to in order to facilitate onward notification of data erasure	High	- Procedure note to be drafted - recording mechanism to be put in	Mar-18	15%
	R43	Identify where R2BF requests may come from. Introduce a R2BF policy and procedures which can identify and erase data as appropriate. Introduce a process which ensures the Councils are able to identify and log any such request and execute it in a timely manner.		See R42		