1 GDPR AUDIT CHECKLIST

GENERAL DATA PROTECTION REGULATION AUDIT CHECKLIST		
LEAD AUDITOR:	**Rob Shelvey**	***DIRECTIONS:*** *1. Answer each requirement based on your current process* *2. Refer to the relevant GDPR Article if you need further clarification on meeting the standard or requirement (if the question relates to a specific Article, it is noted to the left of the question – those without Article references are suggested requirements or guidelines from the ICO or WP29)* *3. Use the requirement number on the Action Plan where corrective actions or mitigating controls are required* *4. Where actions are needed, add a review date for re-auditing*
AUDIT DATE:	**18th July 2018**	
AUDIT DESCRIPTION:	**Review of policy and procedure documentation to ensure alignment to GDPR.**	

1. GOVERNANCE & ACCOUNTABILITY								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
1.1	24	78	Do you have a Data Protection Policy?	Yes			Data Protection aspects covered in multiple policies	
1.2			Do you have a Clear Desk Policy?	Yes			Clear desk policy in place	
1.3			Do you have a Remote Access Policy?	Yes			Yes, within the Access Control Policy	

1.4	24	78	Do you have Data Breach Incident & Notification Policy & Procedures?	Yes			Data breach policy and form	
1.5	24	78	Do you have a Records Management & Data Retention Policies?	Yes			Documented record controls in place.	
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
1.6		78	Do you have an Information Security Policy?	Yes			To ISO/IEC 27001 standards	
1.7			Do you have a documented Business Continuity Plan?	Yes			To ISO/IEC 27001 standards	
1.8			Do you have documented procedures for obtaining, processing & storing personal data?	Yes			To ISO/IEC 27001 standards	
1.9	24, 25, 28, 32	74, 77, 78, 81, 83	Have you implemented appropriate technical and organisational measures to protect data & reduce risks?	Yes			To ISO/IEC 27001 standards	
1.10			Have you conducted an Information Audit?	Yes			Information Flow Register Completed	
1.11			***Does your Information Audit contain: -*** • What personal data you hold? • Where it came from? • Who you share it with? • Legal basis for processing it? • What format(s) is it in?	Yes				

			• Who is responsible for it?					
1.12	4, 24, 28	74, 81	Have you assessed and documented whether you are a *'Data Controller'*, *'Data Processor'* or both?	Yes			Both	
1.13	25, 40, 42, 43	98, 99, 100	If you have obligations under any data protection Codes of Conduct or Certifications, do you disseminate these codes/requirements to all staff?			N/A	No relevant data protection codes of conduct apply.	
1.14			Have your HR policies and procedures been reviewed *(and if applicable, revised)* to ensure that employee's individual rights under the GDPR are considered and complied with?	Yes				
2. DATA PROTECTION OFFICER (DPO)								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
2.1	37	97	Have you allocated responsibility for data protection compliance to a designated person (i.e. *DPO or suitable individual*)?	Yes				
2.2	38	97	Does the Data Protection Officer (DPO) have sufficient access, support and the budget to perform the role?	Yes				
2.3	38	97	Has the DPO identified, created and disseminated reporting lines for the data protection governance structure?	Yes				
2.4	38	97	Are all employees aware of the DPOs appointment & contact details?	Yes				
2.5	38	97	If the DPO has other tasks and duties, have they been assessed to ensure there is no conflict of interest?	Yes				

2.6	37, 39	97	Has the DPO been assessed & verified as having adequate professional qualities and expert knowledge of data protection and the ability to fulfil the tasks referred to below? • To inform and advise the business, management, employees & third parties who carry out processing, of their obligations under the GDPR • To monitor compliance with the GDPR and with the firm's own data protection objectives • Assignment of responsibilities, awareness-raising and training of staff involved in processing operations • To provide advice where requested as regards the data protection impact assessment and monitor its performance • To cooperate with the Supervisory Authority • To act as the contact point for the Supervisory Authority on issues relating to processing	Yes				
2.7	38	97	Is the DPO bound by secrecy and/or confidentiality?	Yes				
2.8	37	97	Have you published the contact details of the Data Protection Officer?	Yes				
2.9	37	97	Have the DPO's contact details been communicated to the Supervisory Authority?	Yes				

2.10	38	97	Does the DPO have access to suitable training materials, courses and workshops to support and improve their role & knowledge?	Yes				
2.11			Have reporting mechanisms been developed between the DPO and senior management?	Yes				
3. PRIVACY BY DESIGN & SECURE PROCESSING								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
3.1			Are daily data backups performed and all back-ups kept in a secure, restricted access location?	Yes			To ISO/IEC 27001 standards	
3.2	24, 25, 28, 32	28,29, 78, 83	Do you utilise pseudonymisation and/or encryption methods to secure personal data?	Yes			To ISO/IEC 27001 standards	
3.3	24, 25, 28, 32	28,29, 78, 83	Do you ensure that pseudonyms and their personal identifiers and/or encryption methods and their secret keys, are always kept separate and secure?	Yes			To ISO/IEC 27001 standards	
3.4	25	78	Do you advocate data minimisation & only obtaining and processing the minimum information necessary for the purpose specified?	Yes			No irrelevant data processed	
3.5	25	78	Is data collected by electronic means (*i.e. forms, website, surveys etc*) minimised so only the relevant fields are used, as relevant to the processing purpose?	Yes			No irrelevant data processed	

3.6	24, 25	78	Do you have documented destruction procedures in place for information that is no longer necessary, surplus to requirement or part of an individual's consent withdrawal or right to erasure?	Yes			To ISO/IEC 27001 standards	
3.7	24, 25	78	If you must use hard copy data for storing or processing, do you use redaction methods where possible to ensure data minimisation?	Yes			To ISO/IEC 27001 standards	
3.8			Do you enforce strong passwords across your organisation?	Yes			To ISO/IEC 27001 standards	
3.9			Are passwords to networks, computers and backups changed every 30 days?	Yes			To ISO/IEC 27001 standards	
3.10	24, 25	78	Do you restrict access to personal information to only those employees processing the data?	Yes			To ISO/IEC 27001 standards	
3.11	25, 32	78, 83	Do you activate strong security defaults on all systems and networks?	Yes			To ISO/IEC 27001 standards	
3.12	32	83	Do you carry out frequent audits & reviews to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services?	Yes			To ISO/IEC 27001 standards	
3.13			Do you have documented; robust & tested business continuity plans to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident?	Yes			To ISO/IEC 27001 standards	

3.14	24, 25, 32	83	Do you have a documented audit & review process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing?	Yes			To ISO/IEC 27001 standards	
4. PRINCIPLES & PROCESSING ACTIVITIES								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
4.1	5	39, 60	***Is personal information: -*** • processed lawfully, fairly and in a transparent manner? • collected for specified, explicit and legitimate purposes only? • adequate, relevant and limited to what is necessary? • accurate and, where necessary, kept up to date • kept only for as long as is necessary and only for the purpose(s) which it is processed? • processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage?	Yes			Evidenced by privacy policy and information flow register.	
4.2	32	75, 76, 77	Have you carried out a risk assessment to identify, assess, measure and monitor the impact(s) of processing?	Yes			To ISO/IEC 27001 standards	
4.3	30, 32	82	Do you carry out internal audits of all processing activities?	Yes			To ISO/IEC 27001 standards	

4.4	6	40-50	Do you identify and establish the legal basis for all personal data that you process?	Yes			Documented within information flow register	
4.5	9	51-56	If you process special category, is it in compliance with one or more of the Article 9(2) conditions?	Yes				
4.6a	30	13, 82	***If you employee <u>less</u> than 250 people, do you maintain records of all processing activities where: -*** • Processing personal data could result in a risk to the rights and freedoms of individual? • The processing is not occasional? • You process special categories of data or criminal convictions and offences?	Yes			Documented within information flow register	
4.6b	30	82	***If you employee <u>more</u> than 250 people and act in the capacity as a <u>controller</u> (or a representative), do your internal records of the processing activities carried contain: -*** • Your full name and contact details and the name and contact details of the Data Protection Officer? • Where applicable, details of any joint controller and/or the controller's representative? • The purposes of the processing? • A description of the categories of data subjects and of the categories of personal data? • The categories of recipients to whom the personal data			N/A		

			has or will be disclosed *(including any recipients in third countries or international organisations*)? • Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)? • Where possible, the envisaged time limits for erasure of the different categories of data? • A general description of the processing security measures you have in place?					
4.6c	30	82	***If you act in the capacity as a <u>processor</u> (or a representative) <u>on behalf of a controller</u>, do your internal records of the categories of processing activities carried out, contain: -*** • Your full name and contact details? • The full name and contact details of each controller on behalf of which you are acting? • The name and contact details of the Data Protection Officer? • The categories of processing carried out on behalf of each controller • Where applicable, transfers of personal data to a third country or an international organisation (including the	Yes			Controller details held internally. Security and safeguarding measures within privacy and security policies.	

			identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)? • A general description of the processing security measures you have in place?					
4.7	30	82	***Do you ensure that the above records are: -*** • maintained in writing? • provided in a clear and easy to read format? • readily available to the Supervisory Authority upon request?	Yes			Terms and contracts	
4.8	6	40-50	Prior to obtaining & processing personal information, do you carry out a review to verify compliance with one or more of the lawfulness of processing conditions?	Yes			Documented within information flow register	
5. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
5.1	35	84, 90	When processing is likely to be high risk or cause significant impact to a data subject, do you carry out Data Protection Impact Assessments (DPIA)?			N/A	Many internal risk and impact assessments are carried out under ISO/IEC 27001 relating to the security of systems and data. Be Software International Pty Ltd are not a controller of any high risk	

							personal data and therefore cannot make impact assessments on any high risk data they process for data controllers.	
5.2	35	84, 90	Do you have a process and screening questions for determining whether a DPIA is required?			N/A		
5.3	35	84, 90	Does this process utilise the Article 35 definitions of high risk processing?			N/A		
5.4	24		Do you have documented policies & procedures for completing a DPIA?			N/A		
5.5	35, 39		Is the DPO always involved in the assessment and mitigating action plan?			N/A		
5.6	35	90	***Does the DPIA contain: -*** • A systematic description of the envisaged processing operations? • The purposes of the processing? • Where applicable, the legitimate interest pursued by the controller? • An assessment of the necessity and proportionality of the processing operations in relation to the purposes? • An assessment of the risks to the rights and freedoms of			N/A		

			data subjects? • The measures envisaged to address the risks *(inc. safeguards, security measures and mechanisms to ensure the protection of personal data)*?					
5.7	35		Where appropriate, do you seek the views of data subjects or their representatives on the intended processing?			N/A		
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
5.8	35, 36	90	Are mitigating measures proposed & actioned to reduce the impact of the risk?			N/A		
5.9			Are all DPIAs documented in writing?			N/A		
5.10	35		Where there is a change to the risk posed by processing, is a review of the DPIA carried out?			N/A		
5.11	36	94, 96	Where measures fail, or cannot mitigate the risk, do you consult the Supervisory Authority prior to processing where a DPIA indicates that the processing would result in a high risk?			N/A		
5.12	36	94, 96	***If consulting the Supervisory Authority, do you provide: -*** • The respective responsibilities of the controller *(if applicable)*? • Joint controllers and processors involved in the			N/A		

			processing *(if applicable)?* • The purposes and means of the intended processing? • The measures and safeguards provided to protect the rights and freedoms of data subjects? • The contact details of the Data Protection Officer? • The data protection impact assessment? • Any other information upon request?					
6. CONSENT & INFORMATION DISCLOSURES								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
6.1	7	32, 42, 43	Are you always able to demonstrate that consent has been given?	Yes			Details within privacy policy	
6.2	7, 12	32, 42, 60	Where processing is based on consent, is the request in a clear and transparent format, using plain language and avoiding any illegible terms or jargon?	Yes			Details within privacy policy	
6.3	7, 12	42	Is the request in an easily accessible format with the purpose for data processing attached to that consent?	Yes			Details within privacy policy	
6.4	7	42	Where consent is requested in the context of a written declaration which also concerns other matters, is the request always presented in a manner which is clearly distinguishable	Yes			Details within privacy policy	

			from the other matters?					
6.5	7, 17	42, 65	Is the data subjects' right to withdraw consent at any time made clear?	Yes			Details within privacy policy	
6.6	7	42, 65	Is the process for withdrawing consent simple, accessible and quick?	Yes			Details within privacy policy	
6.7	8	38	Where personal information is obtained and/or processed relating to a child under 16 years (***13 years for DP Bill in UK***), do you ensure that consent is given and documented by the holder of parental responsibility over the child?			N/A		
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
6.8	8, 12	38, 58	Where services are provided to children, does your communication information and privacy notice provide clear & plain information that is easy to understand by a child?			N/A		
6.9			When physically collecting personal information (*i.e. face-to-face, telephone etc*), are supporting scripts used to remind staff of the conditions for consent and an individual's right to be informed?			N/A	Mostly not applicable as very little data is collected by phone or face to face.	
6.10	7		Do you have clear audit trails to evidence consent and where it came from?	Yes			All consent recorded	
6.11	13, 14	42, 60,	Do you utilise a Privacy Notice/Policy (*on your website,*	Yes				

		61	*contracts, emails etc*) to ensure compliance with the conditions for consent and information disclosure rules?					
6.12	13	42, 60, 61	***Where personal data is <u>collected directly</u> from the data subject, do you ensure that the below information is provided at the time of consent: -*** • Identity and contact details of the controller (*or controller's representative)?* • Contact details of the Data Protection Officer? • Purpose of the processing and the legal basis for the processing? • The legitimate interests of the controller or third party? • Any recipient or categories of recipients of the personal data? • Details of transfers to third country and safeguards? • Retention period or criteria used to determine the retention period? • The existence of each of data subject's rights? • The right to withdraw consent at any time, where relevant? • The right to lodge a complaint with a supervisory authority?	Yes			Within privacy policy	

			• Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data? • The existence of automated decision making (*inc profiling*) & information about the logic involved & the significance/envisaged consequences for the data subject?					
6.13	14	61	***Where personal data has <u>not</u> been obtained directly from the data subject, do you ensure, in addition to the above disclosures, that you also provide: -*** • The categories of personal data? • The source the personal data originates from and whether it came from publicly accessible sources?			N/A	All data collected as a controller comes direct from the data subject.	
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
6.14			Do you test, review & audit Privacy Notices to ensure adequacy, effectiveness and data subject understanding?	Yes				
6.15			Are final Privacy Notices authorised by Senior Management/Director and the DPO before being activated?	Yes				
6.16	7, 13,	32	Is the Privacy Notice displayed clearly and prominently?	Yes				

	14							
6.17	7, 13, 14	32	Are individuals asked to positively opt-in?	Yes				
6.18	7, 13, 14	32	Does the Privacy Notice give the individual sufficient information to make an informed choice?	Yes				
6.19	7, 13, 14	32	Does the Privacy Notice explain the different ways that you will be using the personal information?	Yes				
6.20	7, 13, 14	32, 60	Have you provided a clear and simple way for individuals to indicate that they agree to different types of processing?	Yes				
6.21	7, 13, 14	32	Does the Privacy/Consent Notice include a separate unticked opt-in box for direct marketing?	Yes			Whenever consent is required.	
6.22	6, 7, 13, 14	32	Does your Privacy Notice clearly define the lawful basis for processing?	Yes				
7. DATA SUBJECT NOTIFICATIONS, REQUESTS & COMMUNICATION								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
7.1	12	60	Where you act on a data subjects request under Articles 15 to 22, do you provide information on the actions taken in writing *(i.e. data erasures, rectifications etc)*?	Yes				

7.2	12	58, 60	For information disclosures (*Articles 13 & 14*) and communications relating to Articles 15-22 & 34, are responses and information sent to individuals in a concise, transparent, intelligible and easily accessible form?	Yes				
7.3	12	59	Is requested/required information sent free of charge (*unless a specific GDPR requirement states otherwise*)?	Yes			Detailed in subject access request procedure	
7.4	12	59	Is requested/required information sent within 30 days of receiving the data subjects' request/action?	Yes			Detailed in subject access request procedure	
7.5	12	59	Where it is not possible to comply with the 30-day timeframe for responding, do you inform the data subject(s) of the extension within 30 days of receipt of the request, together with the reasons for the delay?	Yes			Detailed in subject access request procedure	
7.6	12	59	If you do not act on a request under a right exemption, do you inform the data subject within 30 days, of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy?	Yes			Detailed in subject access request procedure	
7.7	12	58, 60	Where communicating with a data subject, is the content always clear and using plain language?	Yes			Detailed in subject access request procedure	
7.8	12	58, 60	When requesting access to information or exercising a right, is the information provided to the individual in writing and/or by	Yes			Detailed in subject access request procedure	

			electronic means (*where appropriate*)?					
7.9	12	64	If the data subject requests access to processing information and this is to be provided orally, do you verify the individual's identity by other means first?	Yes			Detailed in subject access request procedure	
7.10			Have you reviewed all existing data subject request processes and timeframes and updated them to comply with the new deadlines and GDPR timeframes?	Yes				
7.11	12, 15	59, 63	Do you have dedicated procedures for handling subject access requests and request refusals?	Yes			Detailed in subject access request procedure	
8. DATA SUBJECT RIGHTS								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
8.1	15	63, 64	***Where a data subject exercises their Right of Access, do you ensure that they are provided with: -*** • The purposes of the processing? • The categories of personal data concerned • The recipients or categories of recipient to whom the personal data has/will be disclosed? • Whether the personal data has/will be transferred to a third countries or international organisations? • Pursuant to the above, the right to be informed of the	Yes			Detailed in subject access request procedure	

			appropriate safeguards used? • The envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period? • The existence of the right to request rectification or erasure of personal data? • The existence of the right to restrict processing of personal data or to object to such processing? • The right to lodge a complaint with a supervisory authority? • Where the personal data was not collected directly from the data subject, information as to the source? • The existence of automated decision-making *(inc. profiling*) and details of the logic involved, as well as any significant/envisaged consequences of such processing?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
8.2	16	65	Do you have a process for rectifying inaccurate personal data and/or completing incomplete personal data completed *(inc supplementary statements*)?	Yes			Detailed in subject access request procedure	
8.3	17	65, 66	***Where a data subject exercises their Right to Erasure, do you check the request against the below list before complying?***	Yes			Detailed in subject access request procedure	

			• The personal data is no longer necessary in relation to the purposes for which it was collected. • The data subject withdraws consent on which the processing is based. • The personal data has been unlawfully processed. • The personal data must be erased for compliance with a legal obligation. • The personal data has been collected in relation to the offer of information society services. • The data subject objects, on grounds relating to their particular situation, to processing of concerning them which is based on points (e) or (f) of Article 6(1). • The data subject objects to the processing pursuant to data being processed for direct marketing purposes.					
8.4	17	65, 66	Where the data subject has a valid request to have personal data erased and that data has been made public, do you take every reasonable step, to request the erasure by such controllers of any links to, or copy or replication of, those personal data?	Yes			Detailed in subject access request procedure	
8.5	18	67	Where the accuracy of the personal data has been contested by the data subject, do you restrict processing for a period to enable verification of the accuracy of the personal data?	Yes			Detailed in subject access request procedure	

NO	ARTICLE	RECITAL	REQUIREMENT	YES	NO	N/A	AUDITORS NOTES	REVIEW DATE
8.6	18	67	Where processing is no longer necessary or lawful, do you have a process for restricting processing where requested this over erasure?			N/A	Data deleted if no longer necessary or unlawful.	
8.7	19	66	Do you notify any third party also processing such information about the restriction? *(using the data from your Information Audit)*	Yes				
8.8	21		Where a data subject exercises rights of erasure, objection or rectification, do you restrict processing for a period to enable verification of the validity of the request?	Yes			Detailed in subject access request procedure	
8.9	18	67	Do you ensure that where a data subject has obtained restriction of processing, they are informed in writing before the restriction is lifted?	Yes			Detailed in subject access request procedure	
8.10	20	68	Where possible, do you retain copies of personal data in a structured, commonly used and machine-readable format to comply with the Right to Data Portability?	Yes			Converted upon request.	
8.11	20	68	If requested by a data subject, do you transmit personal data to another controller in a machine-readable format?	Yes				
8.12	22	71, 72	Do you avoid using solely automated processing (*inc profiling*) in your decision-making processes, unless consent has been given by the data subject?	Yes				

8.13	12	59	Do you have procedures and controls in place to ensure that all personal information can be provided electronically?	Yes			Detailed in subject access request procedure	
8.14	21	70	Can individuals object to having their personal information processed for direct marketing?	Yes				
9. TRANSFERS, SHARING & THIRD PARTIES								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
9.1	28	81	If you use a third party to process any personal information (*e.g. I.T Services, HR Providers etc*), do you carry out due diligence checks prior to selection?	Yes			To ISO/IEC 27001 standards	
9.2	28, 32	81	***Do you have compliant Service Level Agreements (SLAs) and contracts with each third party processor, which outline: -*** • Required skill, competency and knowledge? • The processors data protection obligations? • Your expectations, rights and obligations? • The processing duration, aims and objectives? • The data subjects' rights and safeguarding measures? • The nature and purpose of the processing? • The type of personal data & categories of data subjects? • Frequency & type of ongoing due diligence & monitoring?	Yes				
9.3	28, 32	81, 83	When transferring or disclosing personal information, do you	Yes			To ISO/IEC 27001 standards	

			encrypt the data and only send what is necessary?					
9.4	32		Do you use secure data transfer methods for communications (*i.e. emails, website forms, online payments*)?	Yes			To ISO/IEC 27001 standards	
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
9.5	28, 32	78, 79, 81, 83	***When sharing or disclosing personal information, do you carry out a data sharing assessment and identify and record: -*** • The benefits and risks of sharing the data • The objectives and goal of sharing • What information needs to be shared • Who requires access to the shared personal data • How should it be shared • Encryption methods and data minimisation tools • How to assess and monitor that the sharing is achieving its objectives? • Due diligence checks of the entity or individual who will receive the personal information?	Yes			No sharing or disclosure of data takes place without consent.	
9.6			Is the DPO (*or appointed suitable individual*) and I.T Manager/Department involved in the setup of any personal data transfers?	Yes				
9.7	45, 46,	101-	**Do you only effect a transfer of personal data to a third**	Yes				

	47, 48	107	**country or international organisation (*outside of the EU*), where one or more of the below conditions applies?** **1.** Where the Commission has decided that the third country/organisation ensures an adequate level of protection (*Adequacy Decision)* **2.** In the absence of an Adequacy Decision, where you have provided appropriate safeguards and have ensured that enforceable data subject rights and effective legal remedies for data subjects are available **3.** With Supervisory Authority authorisation, transfers can take place where there are: - **(a)** Contractual clauses between the controller (*you*) or processor and the controller, processor or the recipient of the personal data in the third country or international organisation? **(b)** Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
9.8	45	101-	Where relying on an Adequacy Decision by the Commission, do	Yes			https://ec.europa.eu/info/law/	

		107	you regularly check notices and publications for withdrawals/changes of decisions?				law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en	
9.9	46, 47	108, 109, 110	Do you ensure that where you are transferring pursuant to appropriate safeguards being in place, as referred to in 9.6; that one or more of the below is used? • A legally binding and enforceable instrument between public authorities or bodies • Binding corporate rules • Standard data protection clauses adopted by the Commission • Standard data protection clauses adopted by a Supervisory Authority and approved by the Commission • An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights • An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the	Yes				

			appropriate safeguards, including as regard data subjects' rights					
9.10	47	110	***Where you rely on binding corporate rules to data transfers outside of the EU, do you ensure that they are: -*** • Legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees? • Expressly confer enforceable rights on data subjects with regards to the processing of their personal data?	Yes				
10. TRAINING & COMPETENCY								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
10.1			Do you educate all employees & management about the GDPR requirements and principles & the possible impact of non-compliance?	Yes			ISMS Training to ISO/IEC 27001 standards	
10.2			Do you have an effective data protection training program in place?	Yes			ISMS Training to ISO/IEC 27001 standards	
10.3			***Does your data protection training program cover: -*** • GDPR scope & principles? • Measures & controls for protecting data & minimising	Yes				

			risks? • Data Protection Officer duties? • Supervisory Authority role and scope? • Codes of Conduct and/or Certifications? • Privacy Impact Assessments (PIA)? • Information Audits? • Processing Activities & Conditions? • Conditions for Consent & Privacy Notices? • Data Subject Rights & subject Access Requests? • Third Country or International Organisation Transfers • Reporting Lines & Notifications? • Privacy by Design (*i.e. data minimisation, pseudonymisation & encryption*)?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
10.4			Do you use assessment testing and/or 1:2:1 mentoring to assess and verify and evidence employee knowledge & understanding of the GDPR?	Yes			Comprehension checks in place	
10.5			Do you provide employees with training evaluation forms so that training is effective and adequate?	Yes				
10.6			Are staff with direct personal data processing duties provided with support, guidance and additional training regarding the	Yes				

			GDPR requirements?					
10.7			Do employees sign confidentiality agreement and/or non-disclosure forms?	Yes				
10.8			Do you have a Training & Development Policy?	Yes				
10.9			Do employees have training records, files and annual training assessments?	Yes				
10.10			Are employees advised of their own rights under the GDPR?	Yes			Where applicable	
10.11			Do you have a GDPR awareness program in place for ensuring that employees understand the new Regulation prior to it coming into effect?			N/A	GDPR now already in place.	
11. AUDITS & MONITORING								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
11.1			Do you have documented Audit & Monitoring Policy & Procedures that have been reviewed within the past 12 months?	Yes			To ISO/IEC 27001 standards	
11.2			Are all GDPR and associated data protection procedures audited at least annually for compliance with the Regulations and you own objectives?	Yes				
11.3			Are employees monitored on an ongoing basis for compliance with the data protection laws *(i.e. email checks, account audits, monitoring phone calls etc)*	Yes				

11.4		84	Are all new processes and/or systems assessed for risks to data protection?	Yes				
11.5			Are processing activities reviewed regularly to ensure they are still valid and effective?	Yes				
11.6			Do you have mechanisms in place to spot check processing activities and staff tasks (*relating to data protection*) to ensure their compliance with your obligations and the GDPR?	Yes				
12. BREACH MANAGEMENT								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
12.1	34	86, 87, 88	Do you have documented data breach procedures?	Yes			Data breach procedure in place	
12.2			Are all staff made aware of the reporting lines for breaches?	Yes				
12.3	34	86, 87, 88	Do you maintain a data breach register and record all breaches, regardless of severity or impact?	Yes				
12.4			Is the breach register reviewed by the DPO monthly to look for patterns or duplicated issues?	Yes				
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
12.5	34	86, 87, 88	Are all breaches investigated and corrective actions taken, regardless of the size or scope?	Yes				

12.6	34	86, 87, 88	Where a data breach has been assessed by the DPO and deemed likely to result in a risk to the rights and freedoms, do you report the breach to the Supervisory Authority within 72 hours?	Yes				
12.7	34	86, 87, 88	***Where notifying the Supervisory Authority, does the report include: -*** • A description of the nature of the personal data breach? • The categories and approximate number of data subjects concerned? • The categories and approximate number of personal data records concerned? • The name and contact details of the Data Protection Officer (or other POC where more information can be obtained)? • Description of the likely consequences of the personal data breach? • Description of the measures taken/proposed to address the personal data breach? • Measures to mitigate any possible adverse effects?	Yes				
12.8	34	86, 87, 88	Are high risk breaches reported to the data subject and the above points covered in a clear & easy to read format?	Yes				
12.9	28, 34	86, 87,	Where you use external processor(s), do you ensure that	Yes				

		88	agreements have provisions for meeting the 72-hour notification deadline if there is a breach?					

TO BE COMPLETED BY THE AUDITOR

Have all questions been completed?	YES	**Print Name:**	Rob Shelvey
Have all next review/action dates been set?	N/A	**Signed:**	

GENERAL DATA PROTECTION REGULATION (GDPR) IMPLEMENTATION ACTION PLAN						
CHECKLIST NO.	**SUMMARY**	**CORRECTIVE ACTION OR MITIGATING CONTROL**	**RESPONSIBLE PERSON**	**STATUS**	**DUE DATE**	**COMPLETED (√)**