Questionnaire for GDPR implementation on 25 May 2018

Company/Controller	Receipt stamp Bavarian DPA

I. Structure and responsibility in the company	
1.	▪ Is there an awareness in the company that data protection is management responsibility, e.g. by ▪ Existence of data protection guidelines ▪ Description of the data protection goals ▪ Regulation of responsibilities ▪ Awareness of data protection risks ▪ Transparency of conflicts of objectives (e.g. between the marketing and the legal department)
2.	▪ Does your company have a data protection officer? ▪ If not, why not? ▪ If yes, is it clear in which cases he will be involved by whom? ▪ If yes, has he already been reported to the competent supervisory authority according to Art. 37 para. 7 GDPR?
II. Overview of processing activities	
1.	▪ Do you have records of your processing activities according to Art. 30 GDPR? ▪ If not, why not? Is this documented? ▪ How did you ensure that data protection issues are taken into account within your company upon commencement or modification of each processing activity (Privacy by Design – Art. 25 GDPR)?
III. Involvement of third parties	
1.	▪ Do you engage third parties for the execution of your activities (processors)? ▪ If yes, do you have an overview of your processors? ▪ If yes, have you entered into the necessary agreements containing the minimum content of Art. 28 para. 3 GDPR with all your processors?
IV. Transparency, information duties and assurance of data subject rights	
1.	▪ Have you adapted your texts providing information regarding data protection for data subjects in the course of data collection to the requirements of Art. 13 and 14 GDPR? ▪ If not, why not?
2.	▪ Have you recently included in particular the following information, provided it had not been included before: ▪ Contact details of the data protection officer ▪ Legal basis for processing of personal data ▪ If the purpose for processing data on your behalf or on behalf of third parties lies on legitimate interests: specify the legitimate interests ▪ If you transfer data to third countries: the appropriate safeguards for the protection of the data applied by you (e.g. standard data protection clauses) ▪ Retention period; if impossible to provide, specify the determination of the storage period. ▪ Existence of the data subject's rights to access, to rectify, to erase, to restrict processing, to object on grounds of the particular situation of the data subject, and to data portability ▪ If the legal basis for processing is consent: does the data subject has the right to withdraw the consent at any time ▪ Right to lodge a complaint with a supervisory authority ▪ Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract ▪ If relevant: the execution of automated decision making, including profiling, and, in this case, information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

	▪ If you have not obtained personal data from the data subject: from which source the personal data originates, and if applicable, if it comes from publicly accessible sources ▪ Have you adapted your marketing consents for customers, prospective customers etc. to the requirements of Art. 7 and Art. 13 GDPR (in particular: extended information duties, also regarding the right to withdraw the consent at any time)?
3.	▪ Have you established a procedure in order to promptly and completely satisfy requests for access to the personal data by the data subject according to Art. 15 GDPR (Art. 12 para. 1 GDPR)?
4.	▪ Have you established procedures in order to satisfy requests for data portability by the data subject (Art. 20 GDPR)?
V. Accountability, risk management	
1.	▪ Is there information about each processing activity which serves to prove the lawfulness of processing, e.g. concerning purposes, categories of personal data, recipients and/or deletion periods (Art. 5 para. 2 GDPR)? ▪ Have you assessed if the consents on which your processing is based still complies with the requirements of Art. 7 and/or Art. 8 GDPR?? ▪ Can you demonstrate that consent has been given?
2.	▪ Have you installed a data protection management system in order to ensure and be able to prove that your processing is in compliance with the GDPR (Art. 24 para.1 GDPR)?
3.	▪ Have you adapted your existing security review processes to the new requirements of Art. 32 GDPR? ▪ Have you, in particular, replaced existing checklists for the selection of technical and organisational measures with a risk-oriented approach based on the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms? ▪ Is an appropriate management system implemented for the regular review, assessment and improvement of security measures? ▪ Are protective measures implemented such as pseudonymisation and the use of cryptographic procedures for the protection against unauthorised or unlawful processing done by both external and internal "attackers"?
4.	▪ Have you prepared for the possible necessity to conduct a data protection impact assessment? ▪ Have you established an appropriate method in your enterprise for determining if a data protection impact assessment has to be conducted? ▪ Have you established an appropriate risk method in your enterprise for the conduct of a data protection impact assessment? Have you chosen a process for the data protection impact assessment; have you already tested it?
VI. Data breaches	
1.	▪ Have you ensured that the notification of a personal data breach to the supervisory authority can be performed within 72 hours according to Art. 33 GDPR? ▪ Have you ensured in particular that data breaches in your enterprise can be identified? Have you established an appropriate method in your enterprise to determine a risk or a high risk? ▪ Have you established a process on how to handle potential breaches internally? ▪ Have you determined who communicates when and how with the supervisory authority?

Correctness of information provided above is confirmed		
Date	Management	Data protection officer (if applicable)