This is an unofficial translation of the of the German language document "*Fragebogen zur Umsetzung der DS-GVO zum 25. Mai 2018*", published by the Bavarian Data Protection Authority *Landesamt für Datenschutzaufsicht in Bayern*, on 24 May 2017, available at https://www.lda.bayern.de/media/dsgvo_fragebogen.pdf.

C/M/S/ Law.Tax

Questionnaire on the implementation of the GDPR on 25 May 2018

Company/Controller	Date stamp BayLDA

I. Structure and accountability in the company	
1.	▪ Is your company aware that privacy is a top priority, demonstrated for example by your company's ▪ Existence of data protection guidelines ▪ Description of data protection goals ▪ Regulation of responsibilities ▪ Awareness of privacy-related risks ▪ Transparency of trade-offs (e.g. between marketing and legal department)
2.	▪ Does your company have a data protection officer? ▪ If not, why not? ▪ If so, is it sufficiently clear when and by whom the data protection officer has to be involved? ▪ If so, have the data protection officer's contact details already been communicated to the supervisory authority in accordance with Art. 37 (7) GDPR?
II. Overview of processing operations	
1.	▪ Do you have a record of processing activities pursuant to Art. 30 GDPR? ▪ If not, why not? Is this documented? ▪ How did you ensure that data protection interests are taken into account when initiating or changing processes in your company (privacy by design, Art. 25 GDPR)?
III. Involvement of third parties	
1.	▪ Did you engage third parties (processors) in the handling of processing operations? ▪ If so, do you have an overview of the processors? ▪ If so, do you have an agreement in place with all processors, with the minimum content set out in Art. 28 (3) GDPR?
IV. Transparency, information requirements, and ensuring the rights of the data subject	
1.	▪ Did you update your texts on data protection information for data subjects with the requirements set out in Art. 13 and 14 GDPR? ▪ If not, why not?
2.	▪ In particular, did you add the following information (unless previously included)? ▪ Contact details of the data protection officer ▪ Legal basis for the processing of personal data ▪ Where the processing is based on your legitimate interests or the legitimate interests of a third party, the legitimate interests pursued by you or by the third party ▪ If you are transferring data to third countries: the appropriate or suitable safeguards for the protection of this data (e.g. standard data protection clauses) ▪ The period for which the personal data will be stored; or if that is not possible, the criteria used to determine that period ▪ The existence of the data subject's right to request access to, rectify, and erase personal data, to restrict the processing, to object to processing of personal data on grounds related to the data subject's particular situation, and the right to data portability ▪ Where the processing is based on consent: the right to withdraw consent at any time ▪ The right to lodge a complaint with a supervisory authority ▪ Whether the provision of the personal data is a statutory or contractual requirement or a

	requirement necessary to enter into a contract ▪ If relevant: details regarding automated decision-making, including profiling, and, in such case, information on the logic involved as well as the significance and the envisaged consequences of such processing for the data subject ▪ Where the data have not been obtained from the data subject: from which source the personal data originate, and if applicable, whether it came from publicly accessible sources ▪ Did you update your marketing consent wording for customers, interested parties, etc., to the requirements of Art. 7 and 13 GDPR (in particular any additional information requirements, including the right to withdraw such consent)?
3.	▪ Is there a process in place to address data subjects' requests for access (Art. 15 GDPR) to their personal data in a timely and complete manner (Art. 12 GDPR)?
4.	▪ Is there a process in place to address data subjects' requests for data portability (Art. 20 GDPR)?
V. Responsibility, dealing with risks	
1.	▪ Is there sufficient information to enable you to demonstrate the lawfulness of your processing for each processing activity? For example, regarding purposes, categories of personal data, recipients and/or deletion periods (Article 5 (2) GDPR)? ▪ Did you review whether the consent forms already in use comply with Art. 7 and/or Art. 8 GDPR? ▪ Are you able to demonstrate that the data subject has given consent to the processing operation?
2.	▪ Is there a data protection management system in place to ensure and to be able to demonstrate that the processing is performed in accordance with the GDPR (Art. 24 (1) GDPR)?
3.	▪ Have your existing processes been reviewed in order to comply with the new requirements of Art. 32 GDPR? ▪ In particular, have you replaced existing checklists on the selection of technical and organisational measures with a risk-oriented approach which considers the nature, scope, context, and purpose of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects? ▪ Is there an appropriate management system in place for the regular testing, assessing, and improving of security measures? ▪ Have protective measures such as pseudonymisation and encryption of personal data been implemented to protect against unauthorised or unlawful processing, both with regard to external and internal "attacks"?
4.	▪ Did you prepare yourself for the possible need to carry out a data protection impact assessment? ▪ Did you implement an appropriate method for determining whether a data protection impact assessment is required? ▪ Did you implement an appropriate risk method to carry out a data protection impact assessment in your company? Have you chosen a process for the data protection impact assessment? Have you already tested it?
VI. Data breaches	
1.	▪ Did you – pursuant to Art. 33 GDPR – ensure that the notification of a personal data breach to the supervisory authority is possible within 72 hours? In particular, did you ensure that data breaches are detected in your company? Is there a suitable method for identifying risks and a high risks in your company? ▪ Is there a process in place for dealing with data incidents internally? ▪ Did you determine who, when, and how to communicate with the supervisory authority?

Confirmed		
Date	Management	Data Protection Officer