# Primary changes in the SURF Model Processor Agreement 3.0

**General Notes**

- Both the SURF Model Processor Agreement 2.0 (hereinafter referred to as the '*Model PA 2.0*') and the SURF Model Processor Agreement 3.0 (hereinafter referred to as the '*Model PA 3.0*') incorporate the statutory requirements of the General Data Protection Regulation (hereinafter referred to as the '*GDPR*'). Both models can generally be used under the GDPR. This document discusses the main differences between the documents.
- The Model PA 3.0 is more compact and features a better balance between the interests of the supplier (Processor) and those of the Controller (Institution).

**Article 1. Definitions** *(old Model PA 2.0: Article 1*)

- Definitions already included in the GDPR have been deleted.
- Where necessary, definitions have been clarified and brought into line with the terminology used in the GDPR.

**Article 2. Object of the Processing Agreement** (*old Model PA 2.0: Article 2*)

- The old Article 3 of the Model PA 2.0 has been moved to the new Article 2.3.2.

**Article 3. Provision of Assistance and Cooperation** (*old Model PA 2.0: Article 4*)

- The Processor's obligation to provide assistance to the Controller is limited to assistance that relates to the Processing of Personal Data for the performance of the (main) Agreement.

**Article 4. Access to Personal Data** *(old Model PA 2.0: Article 5*)

- If general Written permission has been given to engage Sub-processors, the Controller has one month to object to the Processor's intended change. The Model PA 2.0 did not contain a maximum term for the objection.
- The provision concerning the Processor passing on its obligations under the Processor Agreement is limited to Sub-processors. Employees only need to be subjected to a confidentiality agreement.
- In the new Article, all that is required is proof that the Processor has passed on the obligations to Sub-processors; access to the Sub-processor agreement is no longer requested. There is no need for access and, moreover, this is often impossible under the applicable confidentiality provisions.

**Article 5. Security** *(old Model PA 2.0: Article 6*)

- Access to the Processor's written security policy will no longer be requested; only proof of the written security policy.

**Article 6. Audit** *(old Model PA 2.0: Article 7*)

- The scope of the audit to be carried out by the Processor only relates to the Processor Agreement, the GDPR and other applicable laws and regulations, and no longer to the (main) Agreement.

- In addition to one being required in the situation in which Special Personal Data is processed, an annual periodic audit by the Processor is also mandatory if the Processing poses a high risk to the rights and freedoms of the Data Subjects.
- The Controller's option to have his own audit carried out at the Processor is subject to more conditions.

**Article 7. Personal Data Breach** *(old Model PA 2.0: Article 8*)

- The Processor's obligation to report a Personal Data Breach no longer covers a reasonable suspicion of a Breach.
- Annex C of the old Model PA 2.0 has been removed. Instead, reference is now made to the Dutch Data Protection Authority's most recent data breach form.

**Article 8. Transfer of Personal Data** *(old Model PA 2.0: Article 9*)

- Reference is made to the articles of the GDPR on the transfer requirements to countries outside the EEA. These requirements are no longer set out in the Processor Agreement itself.

**Article 9. Confidentiality of the Personal Data** *(old Model PA 2.0: Article 10*)

- The provision on the confidentiality of Personal Data has been amended so that legislation and judicial decisions of countries *outside* the EEA are no longer exceptions to the principle of confidentiality. A supplier can now only invoke this exception when it comes to Union or Member State law or court orders. This concerns, for example, actual or potential legislation such as the Cloud Act, which is thus (potentially) kept out.

**Article 10. Liability** *(old Model PA 2.0: Article 11: Liability and Indemnity*)

- The liability provision has been amended and now dovetails with the liability provision in the 'Generic Model Processor Agreement 3.0' of the MBO's Information Security and Privacy Framework.
- The liability provision of the (main) Agreement is now adhered to. In a limited number of situations, this possible limitation of liability under the (main) Agreement does not apply to non-compliance under the Processor Agreement.
- The indemnification provision has been removed.
- The obligation for the Processor to maintain adequate insurance has been removed.

**Article 11. Amendments** *(old Model PA 2.0: Article 12*)

- Amendments to Annex B to the Processor Agreement also require the prior Written consent of the Controller. These concern changes in the security of the Processing.
- Immediately necessary corrections may be made by the Processor without the prior Written consent of the Controller.

**Article 12. Term and Termination** *(old Model PA 2.0: Article 13*)

- The Controller's ability to terminate the Processor Agreement has been included.

**Article 13. Applicable Law and Dispute Resolution** (*old Model PA 2.0: Article 14*)

- The provision concerning the return of the Personal Data specifies that the transfer is based on an open file format.
- Any additional costs for the additional requirements will be reasonably divided between the Parties.

**Annex B: Security Measures** *(old Model PA 2.0: Annex B*)

- Annex B no longer requests other qualifications of the Processor.