Data Processing Agreement

Covering GDPR data processing, NIS2 supply-chain security, and DORA third-party obligations

27 April 2026

Table of contents

DPA version 2026.05. Effective from 1 May 2026. This version supersedes all prior versions.

This DPA is also available in Danish at https://accelcomply.com/da/dpa. In case of any conflict of interpretation between the English and Danish versions, the Danish version controls (consistent with the Danish governing law in Clause 17.1).

Alignment with Datatilsynet's Standard Databehandleraftale

This DPA is designed to satisfy the substantive requirements of Datatilsynet's standard databehandleraftale (March 2024 version, available at www.datatilsynet.dk). The following differences from the standard template are intentional and documented:

Point	Standard template	This DPA	Reason
Sub-processor notice period	30 days	14 days, extendable to 30 days on written request (Clause 7.5(b))	Operationally faster default; 30-day protection available on request
Insolvency /	Optional (March	Included in Clause	Provides equivalent or

Point	Standard template	This DPA	Reason
beneficiary clause	2024)	7.4(c)-(d) as a per-engagement successor mechanism	stronger protection via a named Substitute
Annex structure	Datatilsynet template structure	Equivalent content in Annexes 1-5; extended to cover DORA (Annex 4) and UK transfers (Annex 5)	Scope extensions; core obligations identical

Any public-sector controller who requires strict template conformity should request a version of this DPA with the 14-day notice period replaced by 30 days; I will provide one on written request within 5 business days.

Who does what under this DPA

You are the Data Controller. You decide why personal data is collected and what it is used for. You are responsible to Datatilsynet and to the people whose data is processed. This DPA does not change that.

I am the Data Processor. I process personal data only because you instruct me to, in the course of delivering the services described in the Engagement Letter. I cannot use your data for my own purposes. I am accountable to you for how I handle it.

This distinction matters: if something goes wrong with personal data I handle on your behalf, I must tell you. You then decide whether and how to tell Datatilsynet and the people affected. I will help you do that.

Executive Summary (for the reader who reads only this page)

This Data Processing Agreement (“DPA”) governs how Accel Comply (Behzad Motaghi, sole trader, Vejle, Denmark) handles personal data when providing IT security advisory, NIS2 readiness, ISO 27001 readiness, cloud cost review, or AI readiness services to a client organisation (“Controller”).

What this DPA does: - Confirms that Accel Comply acts as a Data Processor under GDPR Article 28. - Describes exactly what personal data is processed, why, and on what legal basis. - Lists the current sub-processors and the transfer mechanisms covering US-based tools (EU-US Data Privacy Framework + EU Standard Contractual Clauses, Commission Decision (EU) 2021/914). - I will notify you of any personal data breach within **24 hours** of becoming aware (where you are a NIS2-covered entity) or within **48 hours** (for all other controllers). Both windows are stricter than the GDPR Art. 33(2) baseline of “without undue delay.” For NIS2-covered controllers, the 24-hour window is designed to give you working time before your own Art. 23 early-warning obligation to your national CSIRT falls due — that obligation is yours, not mine. In practice I aim to notify within 2-4 hours. For all other controllers, the 48-hour window gives you time to assess before the GDPR Art. 33(1) 72-

hour controller-to-authority deadline expires. - I commit to concrete, named security measures (Annex 3). - Provides deletion/return of all client data within **30 days** of engagement end.

This DPA supplements and does not replace the engagement letter or master services agreement between the parties.

Governing law: Kingdom of Denmark. **Supervisory authority:** Datatilsynet (www.datatilsynet.dk).

Part A: Main Agreement

---

1. Parties and Recitals

How to complete this DPA

This DPA is a template. It is not effective as a binding agreement until both parties have signed a completed version with all placeholders filled in. The fields requiring completion are:

- Clause 1.1: Controller's full legal name, CVR or company registration number, and registered address.
- Clause 1.2(a): Date of the Engagement Letter and brief description of the services engaged.
- Annex 1: Subject matter and purpose of processing, specific personal data categories, and data subject categories for the engagement.
- Clause 16.1 and Annex 3 §9.1: Insurer name and policy number (stated in each signed Engagement Letter).

Until a completed, signed version exists, this document has no contractual force. Do not treat the published version as an executed DPA.

1.1 The parties to this DPA are:

Data Controller ("Controller")	[CLIENT LEGAL NAME], [CLIENT CVR/ORG NO], [CLIENT ADDRESS] ("you", "the Controller")
Data Processor ("Processor")	Behzad Motaghi, trading as **Accel Comply**, CVR DK37260312, Vejle, Denmark ("I", "Accel Comply", "the Processor")

1.2 Recitals

(a) You have engaged me under an engagement letter or master services agreement dated [DATE] (the "Engagement Letter") to provide [brief service description, e.g., NIS2 readiness assessment services].

(b) In the course of delivering those services, I will process personal data on your behalf. GDPR Article 28 requires that relationship to be documented in a written agreement.

(c) This DPA satisfies that requirement. It is incorporated into and forms part of the Engagement Letter. If this DPA and the Engagement Letter conflict on data protection matters, this DPA wins.

(d) Both parties are committed to processing personal data in accordance with Regulation (EU) 2016/679 ("GDPR") and the Danish Data Protection Act (Databeskyttelsesloven, Act No. 502 of 23 May 2018, as amended).[1]

---

2. Definitions

The following terms bear the meanings assigned to them in GDPR and are reproduced here for convenience:

"DPA": this Data Processing Agreement, including all Annexes, governing my processing of personal data on your behalf.

"Substitute": a qualified IT or information security adviser named in the Engagement Letter to receive a handover of engagement data and deliverables in the circumstances set out in Clause 7.4(c).

"Personal Data" (Personoplysninger): any information relating to an identified or identifiable natural person ("data subject"); Art. 4(1) GDPR.

"Special Category Data" (Følsomme personoplysninger): personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation; Art. 9 GDPR.

"Processing" (Behandling): any operation or set of operations performed on personal data, whether or not by automated means; Art. 4(2) GDPR.

"Data Controller" (Dataansvarlig): the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing; Art. 4(7) GDPR.

"Data Processor" (Databehandler): a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; Art. 4(8) GDPR.

"Sub-processor" (Underdatabehandler): any third party engaged by me to carry out specific processing activities on your personal data; Art. 28(2) GDPR.

"Personal Data Breach" (Brud på persondatasikkerheden): a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data; Art. 4(12) GDPR.

---

1 Databeskyttelsesloven (Act No. 502 of 23 May 2018, last amended). The Danish Act supplements the GDPR in areas where the Regulation grants Member State discretion, including derogations for public authorities, criminal-conviction data, and journalistic purposes. It does not create independent obligations for processors beyond those in the GDPR for commercial B2B advisory contexts. See https://www.datatilsynet.dk/english/the-danish-data-protection-act

"Data Subject" (Registreret): the identified or identifiable natural person to whom personal data relates; Art. 4(1) GDPR.

"Supervisory Authority": Datatilsynet (the Danish Data Protection Agency), Carl Jacobsens Vej 35, 2500 Valby, Denmark.

"SCCs": the Standard Contractual Clauses for the transfer of personal data to third countries annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.[2]

"DPF": the EU-US Data Privacy Framework adequacy decision adopted by the European Commission on 10 July 2023.[3]

"Engagement Letter": the engagement letter or master services agreement governing the services, as referenced in Clause 1.2(a).

"TOMs": Technical and Organisational Measures as described in Annex 3 of this DPA.

"NIS2 Act": the Danish Act on Measures to Ensure a High Level of Cybersecurity (Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau), in force 1 July 2025.

"DORA": Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector, in application from 17 January 2025.

---

3. Scope and Purpose of Processing

3.1 I will only process your personal data:

(a) for the purposes described in Annex 1 (Description of Processing); and

(b) on your documented instructions, including as set out in this DPA and the Engagement Letter.

3.2 I will not process personal data for any other purpose, including for my own commercial purposes (such as marketing, service improvement, or benchmarking), without your prior written consent.

3.3 If I think one of your instructions would break GDPR or Danish data protection law, I will tell you straight away, in writing, stating the grounds. I can pause acting on that instruction while we sort it out, but I will keep following your other lawful instructions.

---

2 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679. Published in OJ L 199, 7.6.2021, pp. 31–61. Available: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj/eng. Module 3 (Processor to Sub-processor) is the operative module for transfers from Accel Comply (Processor) to its operational sub-processors.

3 Commission Implementing Decision (EU) 2023/1795 of 10 July 2023, the EU-US Data Privacy Framework adequacy decision. As of April 2026, the DPF remains in force: the EU General Court dismissed the Latombe challenge on 3 September 2025; Latombe filed an appeal to the CJEU in October 2025, which is pending. The PCLOB lost quorum in January 2025 following politically motivated board removals, raising concerns about the oversight body the CJEU previously relied upon in Schrems II. Parallel SCC coverage is maintained per Clause 9. See https://www.dataprivacyframework.gov. EDPB DPF FAQ updated 15 January 2026.

3.4 Where I process personal data in the context of providing a NIS2 readiness assessment, ISO 27001 readiness assessment, cloud cost review, or AI readiness assessment, the scope is further limited to data reasonably necessary to complete the specific service. I apply data minimisation as a default: if a task can be completed on anonymised or pseudonymised data, I will request that form of data.

3.5 Amendment of instructions. You may change your instructions by written notice that references this DPA and specifies any changes to the scope set out in Annex 1. I will confirm receipt and update Annex 1 accordingly within 5 business days.

---

4. Duration

4.1 This DPA takes effect on the date the Engagement Letter is signed and remains in force for as long as I process personal data on your behalf.

4.2 This DPA ends when the Engagement Letter ends, subject to:

(a) the confidentiality obligations in Clause 7.2, which survive termination indefinitely; and

(b) the deletion/return obligations in Clause 15, which survive for 30 days post-termination.

---

5. Nature and Categories of Personal Data

5.1 I expect to process the following categories of personal data in typical engagements, as further specified in Annex 1:

Category	Typical context	Examples
Employee directory data	Access reviews; IAM audits; user-list extraction for scope mapping	Name, work email, job title, department, system access rights
Vendor / supplier contact data	Third-party risk reviews; supplier security questionnaires	Name, business email, phone number, role/title
Customer personal data	Scoping of customer-facing processes; DPIA assistance	May include name, email, account identifiers, only where strictly necessary for scope
System and network log data	NIS2 readiness; cloud security reviews	Usernames, IP addresses, device identifiers in log files
Authentication data	MFA audit; access control review	Usernames, provisioned MFA method (not credentials)

5.2 Special Category Data. Special Category Data is out of scope under this DPA unless explicitly included in the Engagement Letter, together with any additional safeguards that will apply.

Before commencing an engagement where either party reasonably anticipates that the scope may involve Special Category Data (for example engagements with healthcare providers, social-care organisations, HR-system reviews, or occupational health data), I will raise the Art. 9 classification

explicitly during scoping, document the categories of Special Category Data in Annex 1, and agree the additional safeguards in writing before any such data is accessed. Where the engagement is with a healthcare or social-care organisation, this pre-engagement classification step is mandatory, not optional.

If I inadvertently access Special Category Data during an engagement, I will notify you without delay and will not retain, copy, or further process that data.

5.3 Children's data. Personal data of children (data subjects under 16, or under such other age threshold as applies under Member State law per Art. 8(1) GDPR) is out of scope under this DPA unless explicitly included in the Engagement Letter, together with the additional safeguards that will apply (including parental consent verification where applicable).

---

6. Categories of Data Subjects

Depending on the engagement scope, data subjects may include:

(a) **Your employees:** whose data appears in systems, access reviews, or user directories that I examine.

(b) **Your customers:** natural persons who are customers of yours, where their personal data appears in systems or processes within the engagement scope.

(c) **Your vendors and suppliers:** individual contacts at third-party organisations with whom you have a relationship.

(d) **System administrators and IT staff:** privileged-account holders whose access rights are reviewed as part of a security assessment.

---

7. Processor Obligations

7.1 Processing on documented instructions (Art. 28(3)(a))

I will process personal data only on your documented instructions, except where required to do otherwise by EU or Danish law. If that happens, I will inform you of that legal requirement before processing, unless the law prohibits disclosure on important grounds of public interest.

7.2 Confidentiality of personnel (Art. 28(3)(b))

I will ensure that all persons authorised to process personal data are bound by an appropriate duty of confidentiality. Because Accel Comply is a sole-trader practice, I am the only individual with access to your personal data in the ordinary course of an engagement. This clause extends to any substitute or temporary individual engaged under exceptional circumstances, who must sign a written confidentiality undertaking before gaining access.

7.3 Security measures (Art. 28(3)(c); Art. 32)

I will implement and maintain the Technical and Organisational Measures described in Annex 3. I will review the adequacy of those measures at least annually and, in any event, following any Personal Data Breach or material change to the processing environment.

I acknowledge that the selection and maintenance of security measures is an ongoing obligation.

7.4 Availability, resilience, and business continuity (Art. 32(1)(b)-(c))

(a) I will maintain business continuity measures that protect the availability of your personal data and allow me to restore access following a physical or technical incident.

(b) Client personal data is stored in locations where you can retrieve it without my active involvement, either in systems to which you hold independent access credentials, or in file repositories to which I will provide access details on written request within 24 hours.

(c) For any engagement with fees of DKK 100,000 or more, the Engagement Letter must name a Substitute (as defined in Clause 2: a qualified IT or information security adviser) who will receive a handover of all personal data, deliverables, and working documents in the event I am incapacitated, cease to operate for more than **5 business days**, or become insolvent. For engagements below DKK 100,000, naming a Substitute is recommended but optional; absent a named Substitute, the data is returned to you. The handover includes all engagement deliverables, working documents, access details, and findings to date. The Substitute agrees in writing to be bound by an equivalent confidentiality undertaking before any handover occurs.

(d) If I become insolvent or wind up, you are entitled to request the immediate return or deletion of all personal data held under this DPA, and I undertake to ensure that a handover mechanism is in place as described above. This provision supplements, and in the context of personal data, takes precedence over, any insolvency moratorium on asset transfer.[4]

7.5 Sub-processors (Art. 28(2) and (4))

(a) You grant general written authorisation for me to engage the sub-processors listed in Annex 2 at the time of signing this DPA.

(b) I will not engage a new sub-processor or materially change the role of an existing sub-processor without giving you at least **14 days' prior written notice** (email to your designated contact suffices), identifying the sub-processor's name, country of establishment, and the nature of processing. On your written request before the 14-day clock starts, the notice period is extended to **30 days**.

(c) If you object within 14 days, tell me in writing. I then have a further 14 days to find a solution. If I cannot, you can end the relevant part of the engagement without penalty.

(d) I will, as required by Art. 28(4) and as further interpreted by EDPB Opinion 22/2024 on processor and sub-processor obligations[5], impose on each sub-processor the same data protection obligations as set out in this DPA, by written contract. I remain fully liable to you for the sub-processor's performance of those obligations.

---

4 Datatilsynet's March 2024 update to the standard databehandleraftale made the insolvency/beneficiary clause optional (formerly mandatory), aligning it with EU Commission SCCs 2021/914. The March 2024 update notes that while the clause is optional, controllers remain responsible for ensuring personal data is adequately protected if the processor ceases to operate. See https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/mar/aendring-i-datatilsynets-standarddatabehandleraftale. The per-engagement successor mechanism in Clause 7.4(c) implements a practical alternative to the standard template clause.

(e) I will maintain an up-to-date list of sub-processors and make it available to you on request within 3 business days.

7.6 Data subject rights (Art. 28(3)(e))

I will assist you in responding to requests from data subjects exercising their rights under GDPR Chapter III (including rights of access, rectification, erasure, restriction, portability, and objection). On receiving such a request, I will:

(a) Forward it to you without delay (and in any event within 2 business days);

(b) Provide a copy of any personal data I hold that relates to the data subject, within 5 business days of your written request; and

(c) Not respond directly to the data subject except on your written instruction.

If a data subject contacts me directly to exercise their rights, I will notify you immediately and confirm that I directed the data subject back to you.

7.7 Assistance with security, breaches, and DPIAs (Art. 28(3)(f))

I will assist you in meeting your obligations under Art. 32 (security), Art. 33-34 (breach notification), and Art. 35-36 (data protection impact assessments). On your written request for DPIA assistance, I will, within **10 business days**, provide:

(a) A description of the engagement-specific data flows;

(b) A list of the personal data categories, data subjects, and sub-processors involved;

(c) An assessment of the engagement-specific risks I have identified;

(d) A description of the technical and organisational measures applied to mitigate those risks (cross-referencing Annex 3).

Detailed breach-notification obligations are set out in Clause 11.

7.8 Records of Processing Activities (Art. 30(2))

I will maintain the record of processing activities required under Art. 30(2) GDPR and make it available to you or to Datatilsynet on written request within 5 business days.

7.9 Deletion or return at end of processing (Art. 28(3)(g))

Deletion and return obligations are set out in Clause 15.

7.10 Audit rights (Art. 28(3)(h))

Audit rights are set out in Clause 12.

---

5 EDPB Opinion 22/2024 of 8 October 2024 on certain obligations following from the reliance on processor(s) and sub-processor(s). The Opinion clarifies that controllers retain due-diligence obligations across the full sub-processor chain and that processors must support the controller's ability to fulfil this duty. The disclosure obligations in Clauses 7.5(e) and 9.4 of this DPA are designed to operationalise that controller-side duty. Available: https://www.edpb.europa.eu/system/files/2024-10/edpb_opinion_202422_relianceonprocessors-sub-processors_en.pdf

7.11 No use of personal data for AI/ML model training

(a) I will not use your personal data, or permit my sub-processors to use your personal data, to train, fine-tune, or evaluate any artificial intelligence or machine learning model, except where I am directly instructed by you in writing to do so for a specific engagement purpose (for example, where the engagement itself is your own AI readiness assessment and your data is used to test a defined model).

(b) I confirm that the sub-processors listed in Annex 2 are configured, in the contractual settings I have selected, not to use your personal data for training generic AI/ML models for the sub-processor's own benefit. Where a sub-processor offers an opt-in for AI training, I am opted out. I will re-confirm this configuration annually and following any material change to a sub-processor's terms.

(c) Where I use generative AI tools (including large language models) in producing engagement deliverables, I will disclose in the Engagement Letter the tool name, the categories of input I provide to that tool, and the data-handling commitments made by the tool provider. I will not provide your personal data to such tools as input unless explicitly authorised in the Engagement Letter.

(d) This clause supplements, and does not replace, any AI-specific obligations under the EU AI Act (Regulation (EU) 2024/1689) that apply to either party. For the purposes of the EU AI Act, I act as a **deployer** of AI systems provided by third-party providers (including any LLM identified in the Engagement Letter). I am not the provider of those AI systems. My obligations as deployer under Art. 26 EU AI Act apply where the AI system is used in a professional context in the course of an engagement.

---

8. Sub-processors

Current sub-processors are listed in Annex 2. The process for engaging new or changed sub-processors is set out in Clause 7.5.

---

9. Cross-Border Transfers

9.1 Transfers to sub-processors established in the United States are covered by:

(a) The **EU-US Data Privacy Framework** (Commission Implementing Decision (EU) 2023/1795, 10 July 2023), where the sub-processor is certified under the DPF program; and

(b) The **EU Standard Contractual Clauses** (Commission Decision (EU) 2021/914, **Module 3: Processor to Sub-processor**), which apply in parallel as an independent transfer mechanism.

If the European Court of Justice invalidates or suspends the DPF, as it did with Safe Harbor (2015) and Privacy Shield (2020), the SCCs continue as the sole operative transfer mechanism without any further action by you and without any amendment to this DPA. I will, within **10 business days** of any such invalidation or suspension, notify you in writing and confirm whether any supplementary

measures (per EDPB Recommendations 01/2020) are required to maintain an essentially equivalent level of protection.

9.2 The correct SCC module for all transfers from me (as Processor) to my operational sub-processors (HubSpot, Microsoft, etc.) is **Module 3 (Processor to Sub-processor)**. This applies throughout this DPA and in Annex 2. Where a sub-processor's own DPA with me applies Module 2 (Controller to Processor), for example where a vendor treats itself as the controller for certain processing, that relationship is documented separately in the relevant footnote.

9.3 No personal data subject to this DPA will be transferred to a third country outside the EEA unless a lawful transfer mechanism under GDPR Chapter V is in place. I will document the applicable mechanism for each sub-processor in Annex 2.

9.4 Transfer Impact Assessment (TIA). For each transfer of personal data to a sub-processor established outside the EEA that relies on SCCs as the operative transfer mechanism (whether as the primary mechanism or as a DPF fallback), I will maintain a documented Transfer Impact Assessment conducted in accordance with EDPB Recommendations 01/2020 on supplementary measures (final version, June 2021)[6] and SCCs Clause 14. The TIA assesses whether the law and practice in the destination country prevents the sub-processor from fulfilling the SCCs. I will make the current TIA available to you on written request within **10 business days**, or within **5 business days** where you flag a regulatory deadline in the request. I will review each TIA annually and immediately following any material change in the transfer context or in the law of the destination country (including any DPF invalidation).[7]

Current TIA outcome (as at the DPA effective date): For transfers to HubSpot (US) and Microsoft (US) under SCCs Module 3 with EU-US DPF co-applicable, I have assessed the US legal environment under the EDPB six-step framework and concluded that, with the supplementary measures in place (EU data centre as primary processing location; contractual prohibitions on US government access broader than legally required; TLS 1.2+ in transit; AES-256 at rest), the sub-processors can fulfil the SCCs and that an essentially equivalent level of protection exists for these specific transfers. The PCLOB quorum issue noted in Footnote [8] has been assessed and does not

6 EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, final version adopted 18 June 2021. The six-step framework for Transfer Impact Assessments is set out in Section II of those Recommendations. Available: https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

7 SCCs 2021/914, Clause 14 requires the parties to warrant that they have no reason to believe that the laws and practices in the destination country prevent the importer from fulfilling the SCCs. This is an ongoing obligation, not a one-time check at signing. The Processor's TIA obligation in Clause 9.4 is the contractual mechanism by which this obligation is operationalised and made available for controller oversight.

8 Commission Implementing Decision (EU) 2023/1795 of 10 July 2023, the EU-US Data Privacy Framework adequacy decision. As of April 2026, the DPF remains in force: the EU General Court dismissed the Latombe challenge on 3 September 2025; Latombe filed an appeal to the CJEU in October 2025, which is pending. The PCLOB lost quorum in January 2025 following politically motivated board removals, raising concerns about the oversight body the CJEU previously relied upon

currently change this outcome, as SCCs remain the operative independent mechanism. If this assessment changes, I will notify you within 10 business days.

9.5 All current sub-processors are based in either the EEA or the United States (the latter under EU-US DPF + SCCs). I do not engage processors in third countries lacking an adequacy decision. If this changes during an engagement, I will notify you under Clause 7.5 (sub-processor change-notification) and obtain or document the relevant transfer mechanism (additional SCCs, derogations under Art. 49 GDPR, or other applicable safeguards) before any data is transferred.

9.6 UK transfers. Where you are subject to UK GDPR (i.e., you are established in the United Kingdom, or personal data of UK-resident data subjects is processed under this DPA), the transfer provisions of the UK GDPR apply independently of EU GDPR. For any transfer of UK personal data to US-based sub-processors listed in Annex 2, the applicable UK transfer mechanism is set out in Annex 5 (UK IDTA / UK Addendum). Annex 5 is triggered automatically when either party identifies that UK personal data is within scope; no further instruction is required.

9.7 Updates to SCCs and adequacy decisions. Where the European Commission issues new or updated Standard Contractual Clauses, or amends Commission Decision (EU) 2021/914, this DPA updates automatically to incorporate the new Clauses from the date the new Clauses are effective, mirroring the auto-update mechanism in Annex 5 §A5.1.2 for the UK Addendum. Where the Commission issues new or amended adequacy decisions affecting any sub-processor, I will notify you under Clause 7.5 within **10 business days**.

---

10. NIS2 Supply-Chain Security

10.1 The obligations in this Clause 10 apply automatically where you are an essential entity or important entity within the meaning of the NIS2 Act (Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, in force 1 July 2025). You warrant at signing whether you are a covered entity. The parties do not need to take any further step to activate these obligations; however, they are disapplied if you are not a NIS2-covered entity.[9]

10.2 NIS2 Art. 21(2)(d) requires essential and important entities to ensure that their direct suppliers and service providers meet adequate cybersecurity standards. The obligations I take on in this Clause 10 are contractual commitments I make to support your compliance with that obligation; they are not obligations NIS2 imposes on me directly as your supplier. Where this Clause 10 applies, I undertake:

---

in Schrems II. Parallel SCC coverage is maintained per Clause 9. See https://www.dataprivacyframework.gov. EDPB DPF FAQ updated 15 January 2026.

9 NIS2 Directive (EU) 2022/2555, Art. 21(2)(d): essential and important entities must implement "supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers." Transposed in Denmark via the NIS2 Act (Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau), in force 1 July 2025. By placing these obligations in the main body with a conditionality carve-out, the DPA structure ensures that a NIS2-covered controller does not need to request activation, the obligations are pre-embedded, satisfying the Art. 21(2)(d) procurement requirement.

(a) To maintain the security measures in Annex 3 at a standard that, risk-proportionately, covers incident response, access control, supply chain, and encryption, supporting your ability to demonstrate supplier-side adequacy under NIS2 Art. 21(2)(d);

(b) To cooperate with any NIS2-mandated security audit or assessment that you are required to conduct of your service providers, and to do so within the audit framework of Clause 12;

(c) To notify you within **24 hours** of becoming aware of any cybersecurity incident on systems I use to deliver your engagement that you may need to assess against your own NIS2 Art. 23 incident-reporting obligation. Your Art. 23 obligation is yours as the essential or important entity; I cannot discharge it on your behalf. The 24-hour notification gives you working time to assess and report. Threat intelligence I encounter during the engagement that does not rise to the significant-incident threshold is shared in a timely manner during normal engagement communications, not under the 24-hour clock. For all other controllers (not covered by NIS2), I will notify you within **48 hours** of becoming aware of a Personal Data Breach, as set out in Clause 11;

(d) To impose equivalent NIS2 supply-chain obligations on any sub-processor whose services I use to deliver your engagement, by written contract;

(e) To disclose to you, on request, the following information to support your criticality classification of me as a supplier: my business continuity posture (including RTO, RPO, backup strategy, and continuity contact as described in Clause 7.4), my dependency map of material fourth-party sub-processors (i.e., sub-processors of my sub-processors relevant to your engagement), and my current vulnerability-management approach and remediation timelines; and

(f) To provide exit and transition assistance as described in Clause 14.4 to support an orderly handover if the engagement ends for any reason.

10.3 Nothing in this Clause 10 limits the obligations in the rest of this DPA, which apply to all controllers regardless of NIS2 status.

10.4 NIS2 status change. If either party becomes aware that your NIS2 classification has changed after the date of signing this DPA, for example because your sector or subsector becomes newly subject to the NIS2 Act, or because you reach the headcount or turnover threshold for essential or important entity status, each party will:

(a) Notify the other in writing within **30 days** of becoming aware of the change;

(b) Jointly re-assess the supply-chain obligations applicable under Art. 21(2)(d) NIS2 within **60 days** of that notification; and

(c) Update the Engagement Letter and this DPA accordingly to reflect any changes to applicable obligations.

This is a mutual obligation. Neither party bears the re-assessment burden alone. If I become aware of a change in your NIS2 status (for example through sector-specific regulatory publications or public notice) before you notify me, I will raise it with you without delay.

11. Personal Data Breach Process

11.1 Definition. A Personal Data Breach is any event meeting the definition in Clause 2 of this DPA. I apply this definition broadly: it includes suspected breaches where I cannot immediately confirm whether personal data was in fact affected.

11.2 Timing. The notification clock starts when I become aware of a confirmed or suspected breach. On becoming aware:

Step 1, Contain (Hour 0-4): Isolate affected systems or data access; prevent further exposure where technically feasible.

Step 2, Notify (Hour 0-24 for NIS2-covered Controllers; Hour 0-48 for all other Controllers): Send written notification to you. My notification obligation to you rests on GDPR Art. 33(2). The 24-hour and 48-hour windows are stricter contractual standards than the statutory "without undue delay" baseline. For NIS2-covered controllers, the 24-hour window gives you working time to assess before your own Art. 23(4)(a) early-warning obligation to your national CSIRT falls due; that obligation is yours as the essential or important entity, and I cannot discharge it on your behalf. For all other controllers, the 48-hour window gives you time to assess and notify Datatilsynet within the GDPR Art. 33(1) 72-hour window.[10]

Step 3, Provide breach particulars. The notification will include, to the extent then known:

(a) A description of the nature of the breach, including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) My name and contact details (Behzad Motaghi, info@accelcomply.com, +45 [phone on request]);

(c) A description of the likely consequences of the breach;

(d) A description of the measures taken or proposed to address the breach and to mitigate its possible adverse effects.

If not all information is available at the time of notification, I will provide what is known and deliver supplements as soon as possible, without waiting for a complete picture to emerge.

10 GDPR Art. 33(2) sets the statutory standard: "Where the personal data breach involves a processor, that processor shall notify the controller without undue delay after becoming aware of a personal data breach." The 24-hour and 48-hour windows in this DPA are stricter contractual standards than Art. 33(2)'s "without undue delay" baseline. They are included to give practical effect to the controller's own downstream obligations: the 24-hour window for NIS2-covered controllers ensures time to file the NIS2 Act Art. 23 early-warning to the national CSIRT; the 48-hour window for all other controllers ensures time to assess before the GDPR Art. 33(1) 72-hour controller-to-authority clock expires. See also Datatilsynet's breach notification guidance at https://www.datatilsynet.dk/english/data-security/personal-data-breach-notifications

11.3 Investigation and cooperation. I will cooperate fully with your investigation and, at your request, with Datatilsynet or any competent authority. I will not communicate with data subjects about the breach except on your written instruction.

11.4 Documentation. I will document all Personal Data Breaches, including those that are not reportable to a supervisory authority, and make that documentation available to you on request.

11.5 Notification does not constitute admission. Notifying you of a breach does not constitute an admission of liability on my part.

---

12. Audit Rights

12.1 Annual self-attestation. Once per calendar year, at no additional charge, I will provide you with:

(a) A written confirmation that the TOMs in Annex 3 remain in place and have been reviewed within the preceding 12 months; and

(b) A summary of any security incidents (including near-misses) and corrective actions taken in the period.

12.2 Document provision. You may request relevant documentation (policies, records, sub-processor DPAs, TIA summaries, Art. 30(2) records) at any time, not limited to once per year. I will provide the requested documentation within 10 business days.

12.3 On-request third-party audit. You may, no more than once per calendar year (or twice per calendar year in the 12 months following a Personal Data Breach), commission a third-party audit of my compliance with this DPA. You will:

(a) Give me at least **30 days' prior written notice**;

(b) Bear the cost of the third-party auditor;

(c) Ensure the auditor is bound by a confidentiality obligation at least equivalent to this DPA;

(d) Limit the audit's scope to the processing activities covered by this DPA.

12.4 Third-party certification as substitute. If I hold a current, third-party-verified certification relevant to the audit scope (for example ISO 27001 or SOC 2 Type II), I may offer that certification and its supporting evidence as a substitute for or supplement to a physical audit, subject to your agreement. **As at the effective date of this DPA, I do not hold ISO 27001 or SOC 2 certification. This clause activates only if and when such certification is obtained and remains current. I will notify you under Clause 7.5 within 10 business days of obtaining or losing any such certification.**

12.5 Cooperation. I will cooperate fully with audits and inspections conducted under this Clause, including providing access to relevant documentation and systems. I may reasonably restrict physical access to facilities where other clients' data is processed, provided I make equivalent documentary evidence available.

12.6 Regulatory audits. The audit rights in this Clause do not limit Datatilsynet's statutory inspection powers under GDPR Art. 58.

---

13. Liability

13.1 My total aggregate liability to you under this DPA, whether in contract, tort, or otherwise, is capped at the **greater of (a) 24 months' fees paid or payable under the relevant Engagement Letter in the 24 months preceding the event giving rise to the claim, or (b) DKK 500,000** (the "DPA Cap"). This cap is a standalone DPA-level cap and applies regardless of any different cap agreed in the Engagement Letter.

13.2 Carve-outs. The DPA Cap does not apply to:

(a) A breach of the confidentiality obligation in Clause 7.2;

(b) Wilful misconduct or gross negligence by me; or

(c) Liability that cannot be limited under mandatory Danish or EU law.

13.3 Datatilsynet fine contribution. Where you pay a regulatory fine or penalty imposed by Datatilsynet that is wholly or partially caused by my breach of this DPA, and provided you have complied with your own GDPR obligations and taken reasonable steps to mitigate the loss, I will contribute to that fine in proportion to the share of fault attributable to me, up to a maximum of the DPA Cap. The parties will determine the proportion of fault by good-faith allocation reflecting Datatilsynet's findings; absent agreement within **60 days** of the fine being levied, the matter is referred to the dispute resolution mechanism in Clause 17.2.

13.4 Sub-processor failures. I am liable to you for the acts and omissions of sub-processors to the same extent as if I had performed the processing directly, subject to the DPA Cap and carve-outs in this Clause.

13.5 Art. 82 contribution right. Where you pay compensation to a data subject under GDPR Art. 82 and that compensation is wholly or partly attributable to my breach of this DPA, I will reimburse you for the portion attributable to my breach. This reimbursement obligation is **not subject to the DPA Cap**: the right of contribution under Art. 82(5) is a mechanism that protects the data subject's effective remedy and cannot be made subject to a contractual cap between the parties without potentially depriving the data subject of full compensation. My liability for my own breach, as established by the competent court or supervisory authority, determines the amount I owe you under this clause. I will cooperate fully with any Art. 82 claim, including sharing documents, attending meetings, and providing information on terms agreed between us, at no charge to you in the first instance.

13.6 Nothing in this DPA limits either party's liability to data subjects or to Datatilsynet.

---

14. Term and Termination

14.1 This DPA ends when the Engagement Letter ends.

14.2 Either party may terminate this DPA immediately on written notice if:

(a) The other party commits a material breach of this DPA and fails to remedy the breach within **14 days** of written notice identifying the breach;

(b) The other party cannot pay its bills when due, enters into administration or liquidation, or ceases to carry on business; or

(c) Continued processing would violate GDPR or other applicable law.

14.3 Termination of this DPA does not release either party from obligations that have accrued before termination.

14.4 Exit assistance. On termination or expiry of the Engagement Letter for any reason, and for a period of **30 days** following termination, I will:

(a) Continue to make available all engagement deliverables and working documents in a standard machine-readable format (CSV, JSON, or as otherwise agreed);

(b) Provide reasonable knowledge-transfer assistance to enable you or your successor provider to continue without disruption;

(c) Delete or return all personal data per Clause 15.

(d) For the purposes of this Clause and Clause 15, "engagement deliverables" means all reports, assessments, plans, recommendations, working papers, data exports, configuration evidence, screenshots, and other documents produced by me in performing the Engagement Letter, in their final and current draft form, in machine-readable format where applicable.

If you are a NIS2-covered entity and the engagement supports a critical function, the exit assistance period is extended to **60 days** on written request.

---

15. Deletion and Return of Personal Data

15.1 On termination or expiry of the Engagement Letter, or earlier on your written request, I will within **30 days**:

(a) Securely delete or return all personal data processed on your behalf (you may specify your preference);

(b) Delete or return all copies, including in backups and sub-processor systems, to the extent I have authority to do so.

15.2 Where you request return, I will provide the data in a standard machine-readable format (CSV, JSON, or as otherwise agreed).

15.3 On your written request, I will provide a written certificate of deletion within **10 business days** of completing deletion, identifying the categories of data deleted and the method used (e.g., secure overwrite, cryptographic erasure).

15.4 I may retain personal data beyond 30 days solely to the extent required by EU or Danish law (e.g., accounting records under the Danish Bookkeeping Act (Bogføringsloven)). In such cases, I will notify you of the retention basis and duration, and will not further process the data for any other purpose.

---

16. Insurance

16.1 I maintain professional indemnity insurance (professionsansvarsforsikring) covering claims arising from errors and omissions in professional advisory services. The standard coverage limit for engagements covered by this DPA is **DKK 5,000,000 per claim**, with insurer name and policy number stated in the Engagement Letter. On written request before signing the Engagement Letter, the limit can be increased (subject to confirmation by my insurer and a corresponding adjustment to the engagement fee to reflect the increased premium and excess); a higher limit applies only when expressly stated in the signed Engagement Letter. Evidence of bound coverage at the agreed limit is provided under Clause 16.3 before processing begins. You may condition engagement under any new contract on written evidence of bound coverage at the limit you require.[11]

16.2 I will notify you within **10 business days** if my professional indemnity coverage lapses or is materially reduced below the level described in Clause 16.1.

16.3 Evidence of current coverage (certificate of insurance or equivalent) is available on written request within 5 business days.

---

17. Governing Law and Jurisdiction

17.1 This DPA is governed by the laws of the Kingdom of Denmark, including the GDPR as incorporated into Danish law and the Danish Data Protection Act.

17.2 Any dispute arising out of or in connection with this DPA is subject to the exclusive jurisdiction of the Danish courts. The primary court of first instance for commercial disputes between businesses is **Sø- og Handelsretten, Copenhagen** (for disputes above DKK 500,000 or between parties agreeing to that court's jurisdiction by this clause). For smaller claims, Retten i Vejle has jurisdiction unless the parties agree otherwise in writing.

17.3 Either party may escalate the matter to Datatilsynet under GDPR Art. 77 before or instead of pursuing court proceedings.

---

11 Datatilsynet's 2026 enforcement focus areas include scrutiny of large data processors and their sub-processor oversight, audit mechanisms, and security measures. While Datatilsynet does not mandate PI insurance in the GDPR framework, procurement standards for Danish industrial and public-sector clients commonly require a minimum of DKK 10M professional indemnity coverage for IT service providers processing personal data. The insurance declaration in this clause satisfies that procurement requirement without constituting a regulatory obligation. See https://www.datatilsynet.dk/afgoerelser/generelt-om-tilsyn/saerlige-fokusomraader-for-datatilsynets-tilsynsaktiviteter-i-2026

18. DORA Addendum Notice (Financial-Services Clients)

Where you are a financial entity subject to DORA, please refer to Annex 4 (DORA Addendum), which forms part of this DPA. Annex 4 addresses the additional contractual requirements under DORA Arts. 28-30 and is operative from the date of signing this DPA.

---

19. Signatures

This DPA is entered into as of the date last signed below. Electronic execution (DocuSign, Adobe Sign, or equivalent) is expressly accepted by both parties.

For the Controller:

Name: _____

Title: _____

Organisation: _____

Date: _____

Signature: _____

For the Processor (Accel Comply / Behzad Motaghi):

Name: Behzad Motaghi

Title: Founder, Accel Comply

Date: _____

Signature: _____

Part B: Annexes

Annex 1: Description of Processing (Art. 28(3) GDPR)

Annex 1 is completed at engagement start as part of the Engagement Letter and forms part of this DPA. The version of Annex 1 in force at any time is the version most recently signed by both parties or attached to the most recent Engagement Letter amendment.

This Annex must be completed or confirmed for each engagement. It may be attached as a separate schedule to the Engagement Letter.

Field	Details
Subject matter of processing	Delivery of [service type, e.g., NIS2 readiness assessment] as described in the Engagement

Field	Details
	Letter
Duration of processing	Ends when the Engagement Letter ends; see Clause 4
Nature of processing	Accessing, reviewing, analysing, and reporting on client data systems and processes; no sale or disclosure to third parties; no automated decision-making with legal effect on data subjects
Purpose of processing	[Insert per engagement, e.g., “To assess the Controller’s current cybersecurity posture and readiness against NIS2 requirements, including reviewing IAM configurations, incident response procedures, and third-party risk management practices”]
Categories of personal data	As listed in Clause 5.1; to be specified further per engagement. Typical: employee names, work email addresses, job titles, access rights logs, system usernames, IP addresses in log files, vendor contact names and email addresses
Categories of data subjects	As listed in Clause 6; typically: Controller’s employees; Controller’s vendor contacts; Controller’s customers (only where within scope)
Special Category Data	None, unless explicitly agreed in the Engagement Letter per Clause 5.2
Automated decision-making	None, I do not carry out automated decision-making or profiling with legal or similarly significant effects on data subjects

Annex 1 Completion and Signature

This Annex 1 is completed as at [DATE] and forms part of the DPA between [CLIENT LEGAL NAME] and Accel Comply (Behzad Motaghi), effective [DATE].

For the Controller: _____ Date: _____

For the Processor: _____ Date: _____

Annex 2: Current Sub-processors

This list is current as of the DPA effective date. Changes are notified under Clause 7.5.

All transfers from me (as Processor) to these sub-processors use **SCC Module 3 (Processor to Sub-processor)** per Commission Decision (EU) 2021/914. Where a sub-processor also holds DPF certification, both mechanisms apply in parallel.

Sub-processor	Country	Role	Personal data categories	Transfer mechanism
HubSpot, Inc.	United States (EU data centre available)	CRM, contact forms, and HubSpot Meetings (booking client and prospect calls), stores client contact information, engagement notes, and meeting metadata	Client contact names, business email addresses, phone numbers, meeting times	EU-US DPF + SCCs (EU 2021/914, **Module 3**). HubSpot DPA, last modified 14 April 2026.[12]
Microsoft Corporation	United States (EU data boundary for M365)	Microsoft 365, email, calendar (Exchange Online), document storage, Microsoft Teams meetings, Entra ID identity	Any personal data in emails, documents, calendar entries, or meeting notes relating to an engagement	EU-US DPF + SCCs (EU 2021/914, **Module 3**). Microsoft M365 DPA April 2025.[13]

Notes: 1. Where a sub-processor offers an EU-based data centre and I have selected EU hosting, the SCC and DPF columns apply only to residual US-side access (support, engineering). EU processing is primary. 2. The above list is current as of the date of signing. I do not currently use Notion, Loom, Google Workspace, Cal.com, or other third-party productivity or scheduling tools that would process client personal data. If a new sub-processor is engaged, it will be added under the change-notification process in Clause 7.5 before any client personal data is transferred. 3. I do not use any sub-processor for the purpose of selling, aggregating, or re-identifying personal data. 4. **AI/ML training opt-out**

12 HubSpot Data Processing Agreement, last modified 14 April 2026, incorporating EU Commission SCC 2021/914 Module 3, and DPF certification. https://legal.hubspot.com/dpa

13 Microsoft Products and Services Data Protection Addendum, April 2025 version (current at https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA as of April 2026), covering EU data boundary and DPF. Module 3 applies where Accel Comply is acting as a Processor and Microsoft is a Sub-processor of client personal data. See also the Hessian Data Protection Commissioner (HBDI) press statement of November 2025 stating that Microsoft 365 can be used in compliance with German data protection law where specified preconditions are met (this is a single Land authority, not a federal-level Datenschutzkonferenz position).

status (per Clause 7.11(b)): HubSpot: I am opted out of any AI training that would use customer content; HubSpot's AI features process client content under contractual confidentiality. Microsoft 365: Microsoft commits in its Products and Services DPA that customer data is not used to train its foundation models, and tenant data is not shared between tenants. I re-confirm both opt-out states annually as part of my Annex 3 §4.4 review. 5. **Tools that are not sub-processors.** I use Apple Passwords (iCloud Keychain) to store my own service credentials only; no client personal data is processed through this tool. I am actively migrating credentials to passkey-based authentication where supported. No third-party tool outside the sub-processors listed above processes client personal data on my behalf.

Annex 3: Technical and Organisational Measures (TOMs) under Art. 32 GDPR

These measures represent my actual, current security baseline. They are reviewed at least annually and updated following any Personal Data Breach or material change.

1. Access Control

1.1 Multi-factor authentication (MFA): Phishing-resistant MFA is enforced on all accounts that can access client data, using FIDO2 security keys or platform passkeys (Apple Touch ID / Face ID, Windows Hello) as the primary factor where supported by the service. Where a service does not yet support phishing-resistant factors, time-based one-time passcodes (TOTP) are used as an interim measure with a documented migration plan. SMS-based and voice-based MFA are not used. Specific configurations:

- Microsoft 365 (Entra ID): passkey or FIDO2 hardware key;
- HubSpot: TOTP via authenticator app (interim, with passkey migration tracked);
- Any cloud console (AWS, Azure, GCP) accessed in the course of an engagement: phishing-resistant MFA where supported, TOTP otherwise.

MFA bypass methods (per-app passwords for legacy protocols, recovery codes that bypass MFA) are disabled.

1.2 Credential management: All service credentials are stored in **Apple Passwords (iCloud Keychain)**, end-to-end encrypted with Apple's zero-knowledge architecture. No passwords are reused across services. Generated passwords are minimum 20 characters random. I am actively migrating credentials to **passkey-based authentication** (passwordless, phishing-resistant) where service providers support it; this reduces the credential-storage attack surface over time. Client personal data is not stored in the credential manager, only my own service credentials.

1.3 Least privilege: Client systems are accessed using the minimum permissions required for the specific task. Privileged access (global admin, root) is used only where unavoidable, and the session is documented in the engagement log.

1.4 Session management: Admin sessions are terminated promptly after use. No persistent privileged sessions are maintained across engagement tasks.

2. Encryption

2.1 Encryption in transit: All communication between me and client systems uses TLS 1.2 or higher. Connections that do not support TLS 1.2+ are not used for transmitting personal data.

2.2 Encryption at rest, endpoint: My primary work device is an Apple MacBook with **FileVault full-disk encryption (AES-256)** enabled. The device is locked when unattended (auto-lock <5 min) and requires biometric (Touch ID) or password unlock. No client personal data is stored on portable removable media (USB drives, SD cards) without equivalent encryption.

2.3 Encryption at rest, cloud storage: Documents and files containing client personal data stored in Microsoft 365 or other cloud services are protected by the provider's at-rest encryption (AES-256 or equivalent), as documented in the sub-processor's DPA. Cloud storage primary regions are configured to EU regions: Microsoft 365 EU Data Boundary; HubSpot EU data centre. Where a sub-processor's residual functions (support, engineering, product telemetry) involve US-side access, those flows are covered by the transfer mechanisms in Clause 9. I will not store primary copies of your personal data outside the EEA without your prior written consent and a documented Transfer Impact Assessment per Clause 9.4.

2.4 Email: Client personal data is not transmitted by unencrypted email where avoidable. For sensitive data transfer (e.g., access review exports), I use password-protected archives, secure file-sharing links (SharePoint, HubSpot file portal), or encrypted transfer methods as appropriate.

3. Device Security

3.1 Managed endpoint: Only my own managed device is used for engagement work. Client data is not processed on shared, personal (non-work), or unmanaged devices.

3.2 Automatic screen lock: The device locks automatically after 5 minutes of inactivity.

3.3 No client data on personal devices: Client personal data is not downloaded to or stored on any personal mobile device (phone, personal tablet). This is a prohibition, encryption of a personal device does not make it an acceptable repository for engagement data.

3.4 Remote wipe capability: I maintain remote-wipe capability for the primary work device via Apple Find My or equivalent MDM, enabling data erasure if the device is lost or stolen.

3.5 Operating system and software updates: Security patches are applied within 14 days of release for the operating system and primary work applications.

4. Security Monitoring and Incident Detection

4.1 Security logging: I retain access logs for cloud services (Microsoft 365 sign-in logs, HubSpot activity logs) and review them for anomalous activity. For engagements classified as high-risk in Annex 1 (including all NIS2-covered controllers and all engagements involving more than 500 data subjects), log review is conducted at least **daily**. For standard engagements, log review is conducted at least **weekly**.

4.2 Breach awareness: I monitor threat-intelligence sources relevant to the sub-processors listed in Annex 2 (e.g., HaveIBeenPwned for credential exposure, vendor security bulletins).

4.3 Incident response: On detecting a suspected incident, I follow the process in Clause 11.2 (Contain; Notify within 24 hours for NIS2 controllers / 48 hours for all others; Provide particulars; Document and cooperate). An incident log is maintained internally.

4.4 Annual security review: I conduct an annual review of these TOMs, documenting any changes and their rationale. The review date and summary findings are available to you on request.

5. Data Minimisation and Retention

5.1 Minimisation at collection: I request only the personal data strictly necessary for the engagement task at hand. Data exports from client systems are scoped to the minimum fields needed.

5.2 Working copies: Working copies of client data (spreadsheets, screenshots, log extracts) are stored only in my designated work environment (Microsoft 365 / cloud storage) and are deleted or returned per Clause 15 at engagement end.

5.3 No shadow copies: I do not create backup copies of client personal data in personal email, personal cloud storage, or any location outside the primary work environment.

6. Physical Security

6.1 Engagement work is conducted from my registered office/work location. My primary work device is not left unattended in public spaces with client data accessible on-screen.

6.2 Physical documents containing client personal data (print-outs, notes) are stored securely and shredded (cross-cut) when no longer needed.

7. Personnel and Confidentiality

7.1 Solo practice: Accel Comply is a sole-trader practice. I am the only person who processes client personal data in the ordinary course of business. There are no permanent employees.

7.2 Exceptional cases: If a substitute (e.g., a subcontractor for maternity/illness cover) is engaged in circumstances where client data access is unavoidable, that person must sign a written confidentiality undertaking and acknowledge these TOMs before any access is granted. You are notified in advance.

7.3 Security awareness: I maintain awareness of current phishing, social-engineering, and business email compromise (BEC) threats as part of professional development.

8. Sub-processor Security Oversight

8.1 Before engaging any new sub-processor, I review the sub-processor's publicly available security documentation (DPA, security whitepaper, certifications, e.g., ISO 27001, SOC 2).

8.2 I confirm that each sub-processor in Annex 2 has either ISO 27001 certification, SOC 2 Type II attestation, or equivalent, and that this remains valid annually.

9. Insurance

9.1 I maintain professional indemnity insurance (professionsansvarsforsikring) covering claims arising from errors and omissions in professional advisory services. Standard coverage is **DKK 5,000,000 per claim**, with insurer name, policy number, and coverage limit stated in each Engagement Letter. A higher limit (e.g., DKK 10,000,000+) is available on written request before

signing the Engagement Letter, subject to insurer confirmation and a corresponding adjustment to engagement fees. Evidence of bound coverage at the agreed limit is provided under Clause 16.3 before processing begins.

Annex 4: DORA Addendum (Financial-Services Clients)

This Annex is operative where you are a financial entity subject to DORA (Regulation (EU) 2022/2554), which entered into application on 17 January 2025. It forms part of this DPA from the date of signing.

A4.1 Scope and Purpose

This Addendum sets out the additional obligations I take on where you are a DORA-regulated financial entity, as required by DORA Arts. 28-30 contractual requirements for ICT third-party service providers.[14]

A4.2 Description of Services and Sub-contracting

A4.2.1 The ICT services provided are described in Annex 1 of the DPA and the Engagement Letter. All changes to scope are documented by written amendment to Annex 1.

A4.2.2 Sub-contracting. I do not sub-contract functions that directly support your critical or important business functions without your prior written approval. Sub-processors used for operational tools (CRM, email, scheduling, as listed in Annex 2) are pre-approved under the general authorisation in Clause 7.5. Any sub-contracting of substantive advisory work requires a separate written agreement between you, me, and the sub-contractor, on terms at least equivalent to this Addendum.

A4.2.3 I will maintain and make available on request a register of sub-contractors used in connection with your engagement, identifying the function, country, and applicable contractual safeguards.

A4.3 Unrestricted Audit and Inspection Rights

A4.3.1 You, any third party you appoint, and any competent authority (including Finanstilsynet and the European Supervisory Authorities) have unrestricted rights of access, inspection, and audit of my business premises, systems, and documentation relevant to the services provided under the Engagement Letter.

---

14 Regulation (EU) 2022/2554 (DORA), in application from 17 January 2025. Arts. 28-30 set out contractual requirements for ICT third-party service providers. The ESAs published final RTS on ICT third-party risk (Regulation 2024/1773) on 17 January 2025; the European Commission rejected draft subcontracting RTS in January 2025 on grounds of scope. The contractual requirements in this Addendum reflect DORA Arts. 28-30 as in force; parties should monitor ESA technical standard developments. See https://www.digital-operational-resilience-act.com/Article_30.html

A4.3.2 These audit rights are not subject to the annual frequency cap in Clause 12.3. Regulatory authorities may exercise their access rights without prior notice. You may exercise your rights on reasonable notice (minimum 5 business days, unless there is reasonable cause for an earlier request).

A4.3.3 I will cooperate fully and without charge with any audit or inspection conducted by you or a competent authority under DORA Art. 30(2)(c).

A4.3.4 I will participate in threat-led penetration testing (TLPT) exercises if required by you under DORA Art. 26, on reasonable notice.

A4.4 Termination Without Notice on Critical Breach

A4.4.1 Notwithstanding Clause 14.2 of this DPA (which provides for a 14-day cure period), you may terminate the Engagement Letter and this DPA immediately on written notice, without any cure period, in any of the following circumstances:

(a) I commit a significant breach of DORA, GDPR, or other applicable financial services regulation affecting the security or integrity of your ICT systems or data;

(b) A competent authority issues a binding decision or order that makes continued performance impossible or unlawful;

(c) I demonstrate material weaknesses in my ICT risk management that I cannot remediate within a period you reasonably specify;

(d) My continued operation as an ICT third-party service provider is incompatible with your regulatory obligations, as determined by you or a competent authority.

A4.4.2 Immediate termination under this clause does not affect any accrued rights or the obligations in Clauses 14.4 and 15.

A4.5 Exit and Transition Assistance

A4.5.1 Following termination or expiry of the Engagement Letter for any reason, I will provide transition assistance for a minimum of **60 days** (extendable by written agreement) to support an orderly migration of services to you or an alternative provider. Transition assistance includes:

(a) Continued availability of all engagement deliverables, working documents, and data in a machine-readable format;

(b) Knowledge transfer and documentation of methodologies, findings, and in-progress work;

(c) Reasonable cooperation with your alternative provider, including answering technical questions;

(d) Return or deletion of your personal data as required by Clause 15.

This exit and transition assistance is provided under DORA Art. 30(2) contractual requirements, which require ICT third-party provider contracts to include provisions that support the financial entity's exit obligations under Art. 28(7) and (8).

A4.5.2 You will bear the cost of transition assistance that extends beyond 60 days, at a day rate agreed in the Engagement Letter. Transition assistance within the first 60 days is included in the engagement fee.

A4.6 Data Recovery and Continuity

A4.6.1 I will implement and test business continuity plans covering the ICT services I provide to you. On request, I will make a summary of those plans available to you.

A4.6.2 For any engagement under this Addendum, the Engagement Letter must name a handover contact (a successor or peer practitioner under Clause 7.4(c)). Naming a handover contact is a precondition of any DORA-regulated engagement under this Addendum. If I become insolvent, incapacitated, or cease to operate, all data processed on your behalf under this DPA is held in locations you can access independently, or will be made available to you within **24 hours** of written request to the named handover contact.

A4.6.3 I will participate in your business continuity and contingency plan testing exercises at reasonable notice, at no additional charge.

A4.7 Incident Reporting to Financial Regulators

A4.7.1 I will notify you within **4 hours** of becoming aware of any ICT incident I classify as major or critical under DORA RTS classification criteria and that I assess as likely to have a significant impact on your ICT systems or data. For all other ICT incidents that do not meet the major or critical threshold but are reportable to you under this DPA, I will notify you within **24 hours**. The 4-hour and 24-hour windows are contractual commitments that supplement DORA's controller-side reporting timelines under Art. 19, giving you time to file your own Art. 19 incident report to Finanstilsynet before your regulatory deadline passes. Where I am temporarily unavailable (sleep, travel, scheduled time off), the windows run from the point at which I am able to direct attention to notification, with a hard outer limit of **12 hours** from the point of awareness. The business continuity provisions of Clause 7.4 apply if I am unavailable for an extended period.

A4.7.2 The notification under A4.7.1 will include, to the extent then known: a description of the incident, affected systems, estimated impact, and the containment steps taken. Supplements will follow as soon as further information is available.

A4.7.3 I will cooperate with any investigation by Finanstilsynet or other competent authority arising from an ICT incident, including providing documentation and access on request.

A4.8 Information Security Standards

A4.8.1 I commit to maintaining information security standards consistent with DORA Art. 9 ICT risk management requirements throughout any engagement with a DORA-regulated entity, proportionate to the nature, scale, and complexity of the services provided, including controls covering confidentiality, integrity, availability, and authentication.

A4.8.2 I will provide you with evidence of my current security posture (e.g., self-attestation, relevant certifications) on request, and will notify you promptly of any material deterioration.

A4.9 Register of ICT Third-Party Arrangements

I acknowledge that you are required to maintain a Register of Information (RoI) of ICT third-party arrangements under DORA Art. 28(2), and to make that information available to competent authorities under Art. 28(3). I will provide the mandatory data fields required by Commission Delegated Regulation (EU) 2024/1771 (the RoI ITS) for your RoI entry covering this engagement, within 10 business days of written request, using the worksheet in §A4.10 below.

A4.10 Register of Information — per-engagement worksheet

Under DORA Art. 28(2) and Commission Delegated Regulation (EU) 2024/1771, you maintain a Register of Information of ICT third-party service arrangements. The table below provides the mandatory fields for the entry covering this engagement. Fields marked [JOINT] are completed jointly by you and me at engagement start.

RoI field	Mandatory per EU 2024/1771	Value for this engagement
Internal reference number	Yes	[ASSIGNED BY YOU]
Name of ICT third-party service provider	Yes	Accel Comply / Behzad Motaghi, CVR DK37260312
Country of establishment	Yes	Denmark
LEI code (if applicable)	Yes	N/A (sole trader, no LEI)
ICT service category (per Annex I, EU 2024/1771)	Yes	[JOINT — typically: IT advisory services / security consulting]
Function supported (critical or important?)	Yes	[JOINT — to be classified by you: is the NIS2/ISO advisory function critical or important to your operations?]
Substitutability assessment	Yes	[JOINT — sole trader; substitutable with moderate effort; successor mechanism in Clause 7.4(c)]
Concentration risk indicator	Yes	[JOINT — low (sole trader; no systemic concentration exposure)]
Start date of arrangement	Yes	[DATE OF ENGAGEMENT LETTER]
Data sensitivity classification	Yes	[JOINT — typically: confidential / limited internal; no critical infrastructure data]
Sub-contractors used	Yes	HubSpot (US), Microsoft (US) — see Annex 2. No sub-contracting of advisory functions without prior

RoI field	Mandatory per EU 2024/1771	Value for this engagement approval per §A4.2.2.
Data storage location	Yes	EU (Microsoft 365 EU Data Boundary; HubSpot EU region)

I will provide any additional information required to complete your RoI entry within 10 business days of written request, including updated sub-contractor details and any changes to the above fields during the engagement.

Annex 5: UK Transfer Addendum

This Annex is operative where you are subject to UK GDPR, that is, where you are established in the United Kingdom, or where personal data of UK-resident data subjects is processed under this DPA. It activates automatically when either party identifies that UK personal data is within scope; no further instruction is required.

A5.1 UK Transfer Mechanism

A5.1.1 For any transfer of UK personal data to sub-processors listed in Annex 2 that are established outside the United Kingdom (including US-based sub-processors), the applicable UK transfer mechanism is the **International Data Transfer Addendum to the EU Commission Standard Contractual Clauses** issued by the UK Information Commissioner's Office (ICO) under s.119A of the Data Protection Act 2018 (the "UK Addendum").[15]

A5.1.2 The UK Addendum is hereby incorporated by reference into this DPA. The parties agree that this DPA incorporates **Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses**. Where the ICO issues a revised Approved Addendum under Section 18, this DPA updates automatically to incorporate that revision without requiring amendment by the parties. The parties further agree that:

(a) The EU SCCs incorporated into this DPA (Clause 9 and Annex 2) are amended by the UK Addendum to cover UK-restricted transfers;

---

15 The International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK ICO under s.119A of the Data Protection Act 2018, version B.1.0, in force 21 March 2022. From 21 March 2024, UK organisations must use either the UK IDTA or the UK Addendum (together with the EU SCCs) for UK-restricted transfers; the transitional period for legacy SCCs ended on that date. The Part 2 Mandatory Clauses are incorporated by reference per the ICO's approved alternative reference wording at A5.1.2 and update automatically under Section 18. See https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/appropriate-safeguards/what-are-standard-data-protection-clauses-the-uk-idta-and-the-addendum/

(b) For the purposes of Table 1 of the UK Addendum: the Exporter is Accel Comply (as Processor acting on your instructions), and the Importer is the relevant sub-processor as listed in Annex 2;

(c) For the purposes of Table 2: the UK Addendum supplements the EU SCCs, Commission Decision (EU) 2021/914, Module 3 (Processor to Sub-processor);

(d) For the purposes of Table 3: the description of transfers is as set out in Annex 1 and Annex 2 of this DPA;

(e) For the purposes of Table 4: neither party may end the UK Addendum as set out in Section 19 of the UK Addendum. This election is consistent with Clause 9.7 of this DPA, which provides for automatic incorporation of updated SCCs and addenda: if the ICO issues a revised Approved Addendum and the auto-update mechanism in §A5.1.2 incorporates it, there is no basis for termination on that ground alone. Either party retains the right to terminate the Engagement Letter on the grounds set out in Clause 14.2 if a revised Addendum imposes materially different obligations that the other party cannot accept.

A5.1.3 Where a sub-processor is also registered under the UK-US Data Bridge (the UK equivalent of the EU-US DPF), both the UK Data Bridge and the UK Addendum apply in parallel as co-existing transfer mechanisms.

A5.2 UK-Specific Breach Notification

Where a Personal Data Breach affects UK personal data, I will notify you within **48 hours** of becoming aware, to allow you to meet the UK GDPR Art. 33 72-hour notification window to the ICO. EU NIS2 does not apply to UK-established entities, so the 24-hour NIS2 carve-out in Clause 10.2(c) does not flow through to UK personal data; UK incident notification obligations are governed by the UK NIS Regulations and UK GDPR.

A5.3 UK Supervisory Authority

For processing activities subject to UK GDPR, the relevant supervisory authority is the Information Commissioner’s Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, United Kingdom (www.ico.org.uk). Nothing in this Annex limits either party’s right to lodge a complaint with the ICO.

A5.4 Data (Use and Access) Act

Where the UK’s Data (Use and Access) Act 2025 (DUA Act, Royal Assent 19 June 2025) results in a commencement order that materially affects the applicable transfer mechanism for UK personal data (including any modifications to the UK IDTA, the UK Addendum, or the UK-US Data Bridge), both parties will review and, if necessary, amend this Annex within 90 days.
