

Checklist II

Choosing additional optional clauses

Document status: In force
Version: March 2025
Document: Checklist II – Choosing additional optional clauses March 2025
Contact: info@digitale-verwaltung-schweiz.ch

Digital Public Services Switzerland

Haus der Kantone

Speichergasse 6

CH-3000 Bern 7

Bern, March 2025



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



KONFERENZ DER KANTONSREGIERUNGEN
CONFÉRENCE DES GOUVERNEMENTS CANTONAUX
CONFERENZA DEI GOVERNI CANTONALI
CONFEDERAZIUN DA LAS REGENZAS CANTUNALAS

Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere



Schweizerischer Gemeindeverband
Association des Communes Suisses
Associazione dei Comuni Svizzeri
Associaziun da las Vischnancas Svizras

Checklist II – Choosing additional optional clauses

DPSS GTC	Topic	CT	Type	Explanation of clause/option	Examples of optional boilerplate for DPSS contract templates	Remarks
A. General provisions						
1.3	Scope and validity	All	Note	Any deviations from the DPSS GTC 2025 must be stated in the contract documents. It is therefore necessary to check on a case-by-case basis whether the standard provisions meet the respective requirements or whether additional deviations are needed.	<i>Placeholders for deviating and supplementary provisions are provided in all DPSS contract templates in the penultimate section under "Special agreements". The boilerplate below should also be included there, if required.</i>	
4.1	Products and services / Specifications	All	CT prov, App	<p>Every DPSS contract template must begin by specifying the exact subject matter of the contract and the goods/services covered by it. Placeholders for this are included in the templates and must be added to as appropriate.</p> <p>However, it is often advisable to define the individual goods/services more precisely in an additional appendix in order to avoid subsequent disputes about the scope of goods/services to be provided. This is particularly recommended if the quote and specifications document do not comprehensively regulate the scope of</p>	<i>Placeholders are included in the respective DPSS contract templates. If necessary, an appendix containing specifications of the contractual goods/services and an appendix concerning the mandate-related processing of personal data must be included and listed in the DPSS contract template under "Appendices".</i>	

				<p>goods/services or if there is a risk of contradictions between these documents.</p> <p>Insofar as the ICT goods/services require personal data processing, the processed personal data or data categories and the purpose of their processing are to be set out in the contract document or in an appendix thereto.</p>		
7.1 and 7.2	Place of data processing	All	Alt	<p>Ensuring data security and compliance with applicable laws when processing personal and other sensitive data is essential, particularly for business-critical tasks and processes. Any deviation from this provision, and in particular processing in countries that do not have an adequate level of data protection, requires careful examination and assurance of compliance with applicable law in relation to the identified need for protection of the processed data. Legal assistance should be sought to this end. The service procurer's obligations as a data owner/data processor must be guaranteed at all times. It may also be necessary to conclude an additional contract regarding data processing (see section 4.1 of the DPSS GTC 2025).</p>	<p><i>Differing provision to be used only in exceptional cases and only after an assessment of the case in question.</i></p> <p>In partial deviation from section 7 of the DPSS GTC, data processing may, by way of exception, take place in [...] as well as in Switzerland and/or a country that has an appropriate level of data protection in accordance with the applicable statutory provisions, provided that all applicable legal and contractual provisions are complied with. In this context, the parties agree on the following additional protective measures required under applicable law: [...].</p>	
8.2	Project organisation	All except WKV 1	CT prov, Opt, App	<p>Any project organisation/project governance structure and the responsible persons and/or bodies and committees must be agreed at contract level in accordance with the DPSS GTC 2025 if this is deemed necessary and appropriate in the</p>	<p>In accordance with section 8.2 of the DPSS GTC 2025, the project organisation/project governance structure is set out in Appendix [...] to this contract.</p>	<p>Already included in WKV 1.</p>

			<p>specific case. The DPSS contract templates already contain a placeholder for contact persons. Project managers can be listed there. In addition, a more detailed project organisation as well as the project method and governance structure and any diagrams and responsibility matrices etc. should be set out in an appendix. This is especially important for project contracts/WKV 1. However, such a clause could also potentially be useful for other DPSS contract templates, such as DLV 2 or more complex operational management structures under WPV 5.</p>	<p><i>The appendix must also be listed in the DPSS contract template under the existing heading "Appendices".</i></p>
8.3	<p>Security check / Need for increased protection</p>	<p>All</p>	<p><i>Opt, App</i></p> <p>Particularly where the contract entails transferring and supporting business-critical tasks and/or involves sensitive data, special agreements may be necessary to better protect against misuse and comply with any existing regulations.</p>	<p>In accordance with section 8.3 of the DPSS GTC 2025, Appendix [...] to this contract sets out further provisions concerning security checks for the staff deployed to perform the contract.</p> <p><i>The appendix must also be listed in the DPSS contract template under the existing heading "Appendices".</i></p>
8.4	<p>Security-related regulations of the service procurer</p>		<p><i>Opt, App</i></p> <p>Security-related regulations of the service procurer, concerning for example access to premises and remote access to systems, must either be communicated in writing in advance or agreed subsequently in writing. To be on the safe side, the contract document may refer to previously communicated regulations or may list them directly. This is preferable to a subsequent agreement.</p>	<p>In accordance with section 8.4 of the DPSS GTC 2025, the provider is expressly obliged to comply with the security-related regulations of the service procurer as set out in [...Add here a reference to the relevant location, e.g. in the call for tenders or specifications document ... / Appendix [...]] "Regulations of the service procurer" / the following list ... List here all</p>

See also the comments on section 16 of the DPSS GTC 2025 below.

regulations with their version number and date and a reference to their location, e.g. online...]

and to ensure that this obligation is imposed on its own employees that it deploys for the contract and, in accordance with section 9.2 of the DPSS GTC 2025, the deployed employees of any third parties engaged.

Any appendix must also be listed in the DPSS contract template under the existing heading "Appendices".

Subsequent agreements on such regulations must be included as an addendum to the contract.

10.1 Documentation All

*Opt,
Alt*

According to the DPSS GTC 2025, the contract may stipulate that documentation must be jointly inspected. The more important the agreed goods/services are, e.g. if they concern business-critical goods/services of the service procurer, the sooner a joint inspection or acceptance of documentation by the service procurer should take place.

In addition, a specific differing provision concerning the language of the documentation may be added (*Opt 3*).

Opt 1 (One-off acceptance for WKV 1, HKV 3 and possibly DLV 2 and SLV 4)

As an addition to section 10.1 of the DPSS GTC 2025, the following documentation must be prepared by the provider and also accepted by the service procurer within 30 days of receipt **[by ...date... / together with delivery of the other contractual goods/services]:**

[...List documents here, e.g.... Operating instructions / User manual / Installation instructions / Operating manual / Training plan / Migration plan]

Opt 2 (Ongoing acceptance for continuing obligations, e.g. for WPV 5 and possibly DLV 2 and SLV 4):

As an addition to section 10.1 of the DPSS GTC 2025, the following documentation must be updated by the provider on an ongoing basis, but at least once a year [and accepted by the service procurer within 30 days of receipt]:

[...List documents here, e.g.... Operating instructions / User manual / Installation instructions / Operating manual / Training plan / Migration plan]

Opt 3 (Language of documentation)

In deviation from section 10.1 of the DPSS GTC 2025, the documentation must be provided in [...Add language(s) here...].

13.4	Invoicing and payment term	All	<i>Alt</i>	The DPSS GTC 2025 stipulate that invoices must be paid within 30 days of receipt or in accordance with an agreed payment plan. This can be deviated from as required.	In deviation from section 13.4 of the DPSS GTC 2025, a payment term of [20/60] days is agreed.
13.6	Adjustments to remuneration during the contract duration	All	<i>Opt, App</i>	If a provision adjusting the remuneration is required in a contract, this can be included in the DPSS contract template or in an appendix on remuneration/commercial matters. This may relate, for example, to an index-based adjustment for inflation. An open remuneration adjustment	As an addition to section 13.6 of the DPSS GTC 2025, the provider shall have the right to adjust the agreed remuneration for the future [to the end of the respective contract year / to the end of the respective three-year contract term] in line with inflation. The provider shall

provision that cannot be specified in advance (e.g. unilateral adjustment at the discretion of one contractual partner or by agreement between the contractual partners) is, in addition to the obvious disadvantage for the service procurer, usually unenforceable in court and should therefore definitely be avoided.

exercise this right by notifying the service procurer by registered letter no later than 2 months before a potential adjustment date.

[In the event of deflation, the service procurer shall be free to demand a reduction in the agreed remuneration, in which case it must submit its request in writing to the provider no later than 2 months before a potential adjustment date.]

The Swiss consumer price index (base 2010 = 100 points) shall be used to calculate the adjustment. Any price adjustment shall be based on the calculation principles of the Federal Statistical Office and its Inflation Calculator. The month prior to the conclusion of the contract shall be used as the initial basis for calculating the inflation rate, and subsequently the index level at the time of the most recent inflation-related adjustment of the remuneration.

If necessary, a "Remuneration" appendix with detailed remuneration provisions must be added and listed in the DPSS contract template under the existing heading "Appendices".

**14.4/1
4.5
Changes to
goods/services
and
continuation of**

All

*Note,
Alt*

The DPSS GTC 2025 state that, as a general rule, contract work shall continue while proposed changes to the goods/services are being reviewed. However, alternative arrangements may also be

Changes to goods/services and deviations from the general rule of continuing contract

work / Addendum to contract				agreed. In the vast majority of cases, though, this will only become relevant once the change(s) has/have been determined, and therefore a general provision at the time of contract conclusion does not seem sensible. Likewise, an addendum to the contract becomes necessary only at the time when a change to the goods/services is agreed.	work must be regulated in a subsequent addendum to the contract.
16.	Further provisions on data protection and information security	All	Opt, App	<p>The DPSS GTC 2025 refer generally to compliance with data protection and data security regulations (see in particular the whole of section 16 of that document). However, there are often special non-disclosure and confidentiality agreements or data security regulations and guidelines to be observed, which must also be included in contracts with the provider. This is often particularly useful or necessary if employees of the provider or employees of any third-party companies it engages are given access to confidential data (e.g. via remote or physical access to systems).</p> <p>Alternatively, the security-related regulations from the above example can also be mentioned here (<i>in Opt 1</i>) or integrated (in the non-disclosure and confidentiality agreement for <i>Opt 2</i>).</p>	<p><i>Opt 1 (Further provisions)</i></p> <p>In accordance with section 16.3 letter b of the DPSS GTC 2025, the provider is expressly obliged to comply with the [...Add here a reference to the relevant location, e.g. in the call for tenders or specifications document... / legal provisions and ordinances ... / guidelines ... / internal regulations ... / recommendations ...].</p> <p><i>Opt 2 (Non-disclosure and confidentiality agreements)</i></p> <p>In accordance with section 15 and section 16.3 letter b of the DPSS GTC 2025, the provider is expressly obliged to comply with the non-disclosure and confidentiality agreement appended as Appendix [...] to this contract document and to ensure that this agreement is signed by its own employees that it deploys for the contract and the deployed employees of any third parties it engages. The service</p>

procurer may request proof of signing from the provider at any time.

The appendix must also be listed in the DPSS contract template under the existing heading "Appendices".

16. Data protection and information security

All

Opt

Section 16 of the DPSS GTC 2025 contains more detailed provisions regarding data protection and information security and specifically also the reporting of security-related incidents (see section 16.5). However, given the growing rate of significant cyberincidents in the 2020s, the need for specific regulations on cybersecurity has increased. For this reason, the Federal Procurement Conference (FPC) has provided public contracting authorities in the Federal Administration with a model contract clause on procedures in the event of cyberattacks. The aim is to encourage contracting parties to protect personal data, information and systems belonging to the public sector in the event of cyberattacks, particularly in the case of security-sensitive activities that are subject to the Information Security Act (ISA).

A similarly detailed clause was deliberately not included in the DPSS GTC 2025 in addition to section 16.5. However, for specific individual cases, an optional provision should be made available here, which can be applied in contracts. The provision is modelled on the requirements of the Federal Office for Buildings and Logistics (FOBL)

X.1 A "cyberattack" within the meaning of this clause is defined as any intentionally triggered event involving the use of IT resources that results in the confidentiality, availability or integrity of personal data and information, or the traceability of its processing, being compromised.

Optional if the ISA or comparable standards under cantonal law apply to the service procurer:

X.X The provider acknowledges that the processing of the service procurer's personal data and information is subject to the Swiss Information Security Act (ISA), including the relevant implementing ordinances, as well as the federal basic ICT security and/or comparable cantonal standards, in addition to data protection law. The provider is thus obliged to observe and comply with the aforementioned standards in addition to data protection law when processing the service procurer's personal data and information. In accordance with section 9.2 of the DPSS GTC

and the FPC, but adapted to the framework of the DPSS GTC 2025.

When assessing whether, in a specific case, cybersecurity and the handling of cyberincidents should be regulated by means of the attached clause, in addition to the provisions of the DPSS GTC 2025, the key factors are: (a) the protection needs and risk analyses of the competent specialist bodies, the classification of information and the security levels of IT resources in the case at hand; (b) whether the contract-related activity is subject to the ISA and/or comparable standards at cantonal level.

In keeping with a security-by-design and -default approach, increased protection needs should be addressed during the tender process, and tenderers should be asked to describe in as much detail as possible how they will implement the requirements and what concrete and detailed measures they intend to take to protect against cyberincidents.

2025, it shall impose these obligations on any subcontractors it engages.

X.X The provider undertakes to adequately protect its information and communication technology resources, in particular applications, information systems and data collections as well as facilities, products and services used for the electronic processing of personal data and information, which have a potential impact on the provision of goods/services to the service procurer and its personal data and information, against cyberattacks in accordance with the latest state of the art and the risk situation.

In this context, the provider shall ensure that (a) the activities predefined by the service procurer are recorded and these records are continuously analysed in order to allow early detection of and defence against cyberattacks; (b) the materialisation of a recognised risk is prevented in an effective manner, its remediation is initiated immediately and the service procurer is informed of this without delay; (c) vulnerabilities discovered before, during or after a cyberattack (i.e. weaknesses or defects in IT resources with the potential to enable or facilitate a cyberattack) are rectified promptly and at no cost to the service procurer.

X.X The provider shall report potentially successful cyberattacks in accordance with section 16.5 of the DPSS GTC 2025.

Alternative to the above clause if the ISA or comparable standards under cantonal law apply to the service procurer:

The provider shall report potentially successful cyberattacks if the confidentiality, integrity, availability, accountability and/or traceability of the service procurer's personal data and information is, directly or indirectly, potentially at risk or actually compromised, or if this was intended. This applies in particular if the IT resources attacked have access to the service procurer's IT resources or if there are indications that these attacks were carried out in preparation for further cyberattacks, or are associated with blackmail, threats or coercion. The provider shall report the type and execution of such a cyberattack, based on an initial analysis, no later than 24 hours after its discovery to the service procurer and the competent bodies appointed under federal and/or cantonal law and shall simultaneously initiate risk mitigation. The parties shall then exchange information on an ongoing basis about the type and execution, possible and actual consequences, and planned and implemented measures. The provider shall

immediately grant the service procurer and any third parties engaged by the service procurer to handle the incident access to analyses, investigation reports and other findings and information (documents, data, log data, objects, etc.) that allow the specific cyberattack and its effects to be analysed and averted and the consequences of the attack to be minimised.

X.X The provider shall furnish the service procurer with suitable supporting documentation on its cybersecurity every six months without being asked to do so and at no cost to the service procurer. If this supporting documentation is deemed insufficient or if there are any indications of deficiencies in cybersecurity, the service procurer may conduct an inspection in accordance with section 16.2 letter f and section 17 of the DPSS GTC 2025.

X.X The provider shall be liable for a contract penalty in accordance with sections 22.1 and 22.2 of the DPSS GTC 2025 if it violates its obligations under this section and/or sections 15 and 16 of the DPSS GTC 2025. In addition, the provider shall be liable for any damage incurred by the service procurer as a result of cyberattacks and non-compliance with the relevant provisions of this section and of the

DPSS GTC 2025 in accordance with section 21 of the DPSS GTC 2025.

16.2 **Surrender in proceedings abroad** Primarily WPV 5 *Opt* Further specification of the general rule in section 16.2 letter g of the DPSS GTC 2025. This is particularly recommended for larger and more complex projects where foreign involvement cannot be ruled out.

X.1 Reporting obligation

Unless otherwise provided for by law, the provider undertakes to inform the service procurer in writing in good time of the occurrence of any of the following events, insofar as they concern information that is processed by the provider in the course of providing the goods/services (reporting obligations):

- (a) the provider is involved in proceedings in which a foreign authority requests the provider to surrender the service procurer's information (receipt of a subpoena or warrant is equivalent to the opening of proceedings);
- (b) a foreign authority requires preservation of the service procurer's information (legal hold or a similar assessment/review of the situation);
- (c) the provider is obliged by court order to surrender the service procurer's information;
- (d) a situation arises which gives reasonable grounds to believe that the provider may become the subject of foreign proceedings. This may be the case, for

example, if an imminent takeover of the provider by a foreign company threatens to enable foreign authorities to demand the surrender of information or if new legislation is enacted abroad allowing a foreign state to access the service procurer's information, such as the US CLOUD Act or similar rules in the US or other jurisdictions.

In the aforementioned cases, the provider shall also inform the service procurer of the legal basis for such requests and the steps already taken by the provider. If the provider was unable to prevent such access or was unable to inform the service procurer in advance, the provider shall inform the service procurer as soon as possible that access has occurred. If the provider has been obliged to maintain secrecy about these matters by the foreign state to the extent permitted by law, it shall inform the service procurer of the disclosure as soon as possible after the obligation to maintain secrecy has lapsed.

X.2 Defence against requests for surrender and inspection

The provider shall take the defence measures available under applicable law in response to all types of official requests for the surrender and/or inspection of the service procurer's information. In particular, it may also have

recourse to legal remedies to ensure that
(a) no legally valid and binding obligations enforcing the surrender of information are created or (b) preparatory measures to create such obligations on the part of the provider or its subcontractors are prevented or remain without effect. The provider shall generally and at all times endeavour to ensure that, in accordance with the applicable law, whenever requests are made to the provider that are not legally valid and not binding, all types of information belonging to the service procurer shall only come into the hands of a foreign authority, if at all, once all available protective measures have been taken.

If a foreign authority demands that the provider surrender the service procurer's data, (a) the provider shall inform the foreign office or authority (insofar as this is permitted by law) that the service procurer, as part of the Swiss federal state system, has an interest in and is entitled to this data and shall inform it of the contact persons at the service procurer; (b) the provider shall require the authority or office to substantiate the conditions for the requested, forced surrender of data by providing the relevant documentation.

To the extent permitted by law, the provider shall work with the service procurer in

determining the content of responses to disclosure requests.

20.1	Warranty / Agreed characteristics	All	CT prov, App	The agreed characteristics are an important preliminary for determining the scope of the warranty. They must be fully and clearly apparent from the respective placeholders to be completed specifying the subject matter of the contract, from any specification appendix or at least from the quote and specifications document.	<i>Placeholders to be filled in to define the characteristics are included in the respective DPSS contract templates for the descriptions of goods/services. If appropriate, a "Specification of contractual goods/services" appendix must be added and listed in the DPSS contract template under the existing heading "Appendices". See also the comments on section 4.1 of the DPSS GTC 2025 above.</i>
20.6	Warranties for third-party products	All	Alt	Any differing warranty provisions for third-party products must be disclosed by the provider and included in the contract document. These provisions must be examined carefully to ensure that they are acceptable and do not jeopardise the purpose of the contract.	In accordance with section 20.6 of the DPSS GTC 2025, the following differing warranty provisions are agreed for the third-party products [...Name of the products concerned...]: [...Terms of differing provisions...].
21.1	Liability for simple negligence	All	Alt	The DPSS GTC 2025 stipulates a liability limit for simple negligence of CHF 1 million per contract, unless otherwise agreed. Make sure to check whether this sum is sufficient in your case. Especially for major continuing obligations lasting many years (operating contracts, maintenance, etc.) or generally for large contracts with remuneration totalling several million Swiss francs, it is easy to set this amount too low.	In deviation from section 21.1 of the DPSS GTC 2025, the liability for simple negligence shall be limited to CHF [...] million [per contract / per contract per year / per claim].

21. Insurance

Opt

With regard to liability, an insurance clause was deliberately not included in the DPSS GTC. However, adequate insurance cover may well be appropriate for specific projects, for example because of the hazardous nature of the activity. However, it is advisable to carry out a risk assessment and classification prior to the tendering process and, during tendering, either to include insurance requirements for the tenderers or to ask tenderers about their specific insurance cover.

Of course, it is still possible to supplement the proposed optional clause with a specific requirement regarding insurance cover (e.g. the amount of the annual limit and the per-claim limits, the need for cyberinsurance).

The provider guarantees that it and its subcontractors will maintain insurance cover for financial loss, personal injury and property damage with a reputable insurer for the entire duration of the contract, in line with the typical risks in its field of activity and in accordance with industry standards. If relevant with regard to the specific provision of goods/services to the service procurer, the provider also confirms that it and its subcontractors are adequately insured against cyber-risks in accordance with industry standards.

The service procurer may request information from the provider about the current insurance cover at any time. In response to such a request, the provider shall be obliged to provide the service procurer, both for itself and, if explicitly requested, also for its subcontractors, with (a) copies of the relevant insurance policies or, alternatively, proof of insurance or a comparable confirmation of cover; (b) evidence of payment of the relevant premiums.

23.1 Assurance of supply period for spare parts and

All

Alt

The DPSS GTC 2025 stipulate a five-year period for assuring the supply of spare parts and/or replacement products. An alternative period may be specified in the contract.

In deviation from section 23.1 of the DPSS GTC 2025, the supply of spare parts and/or replacement products shall be assured for a period of [...] years.

**replacement
products**

24.1 Support upon termination of the contract	All; for WPV 5, insert in section 12	<i>Opt, App</i>	Particularly in the case of continuing obligations, the more that business-critical tasks and processes are transferred to or made dependent on a provider, the more important it is to ensure the continuity of the service procurer's own business activities by making binding arrangements in advance concerning the support services required from the provider. It is often also worth setting out such support services in a separate contract appendix. This must state whether the remuneration for these services is already covered by the existing contract or whether the services are to be paid for at fixed rates.	<p><i>Opt 1 (Reference to appendix)</i></p> <p>As an addition to sections 24.1 and 24.4 of the DPSS GTC 2025, the provider shall be obliged to provide the necessary support upon termination of the contract to ensure the successful transfer of the contractual goods/services to the service procurer itself or a third party designated by it. The details are set out in Appendix [...] "Support services" to this contract document. The services agreed up to and including the contract termination date shall be included in this contract, and no separate remuneration shall be payable for them. Any additional support services required by the service procurer after termination shall be paid for in accordance with the "Support services" appendix.</p> <p><i>The appendix must also be listed in the DPSS contract template under the existing heading "Appendices".</i></p> <p><i>Opt 2 (Simple description)</i></p> <p>As an addition to sections 24.1 and 24.4 of the DPSS GTC 2025, the provider shall be obliged, with a view to termination of the contract, to migrate free of charge all data required for the continuation of the contractual goods/services[, in particular the</p>	If such services become necessary for a WPV 5, they can be integrated into section 12 of the WPV 5 in the optional clause cited there or in the appendix referred to in that section.
--	--------------------------------------	-----------------	--	---	---

following data: ...], to the provider or a third party designated by it in a standard format that is technically easy to adopt [...Define format here if necessary...].

Opt 3 (Generic description if the services are difficult to determine in advance)

Within a reasonable period after termination of the contract, the parties shall, at the request of the service procurer, meet to initiate the steps required to ensure that the services supplied by the provider can be taken over immediately after the end of the contract by the service procurer itself or, depending on the service procurer's requirements, by a replacement supplier ("reverse transition"). In the event of extraordinary termination, these steps shall be initiated without delay after notice of termination.

The parties shall then coordinate their respective proposals and requirements and develop a demigration plan. The demigration plan shall set out the details of the demigration process (in particular specifications, know-how transfer, training by the provider, responsibilities, remuneration, data format). The provider must ensure the implementation of the demigration plan.

The provider shall be entitled to remuneration based on the amount of work performed for all services provided by it in the context of the reverse transition. The amount of the remuneration shall be agreed separately by the parties in the reverse transition plan.

If the demigration process is delayed beyond the contract termination date, the provider undertakes to continue to provide the support services upon termination in return for payment of remuneration (corresponding to the amount of remuneration under the expired contract) until the reverse transition process can be successfully completed.

The provider's obligations shall end only after the successful provision/completion of all the provider services defined and agreed upon in the context of the reverse transition. The provider's obligations shall end only after written confirmation to this effect from the service procurer.

24.4 Termination support and continuing effect

Primarily CLV 6

Opt

Particularly in the case of online services of all kinds, it may be advisable in certain cases and depending on the length or brevity of the agreed notice periods to grant the provider the option of extending the provision of the online services in question beyond the actual

Irrespective of the reason for the termination of this contract, the provider shall be obliged, at the request of the service procurer, to maintain the services provided under this contract on the same terms on a monthly basis for a maximum extension

end of the contract for a limited period ("right to continuing effect"). Such continuing effect or extension of the service provision is intended to give the service procurer enough time to arrange the transition of the services in question to a new provider or a reverse transition to the service procurer itself.

period of 12 months until a transfer to the service procurer or a replacement supplier appointed by the service procurer can take place. For the other support services that the provider will provide in the course of the reverse transition during such an extension period, the relevant provisions of this contract and section 24 of the DPSS GTC 2025 shall apply.

The above obligation shall also apply in the event of premature extraordinary termination of this contract. If such a termination is initiated by the provider, an extension of the service provision beyond the end of the contract shall only be granted if the current and future financial claims of the provider against the service procurer are adequately secured.

25.2 Provider's duties arising from import certificates

All

Opt

In the specific event that import certificates could give rise to obligations on the part of the service procurer, it must be examined whether these can be contractually transferred to the provider. This may be the case, in particular, when software/hardware needs to be imported and exported, and especially in case of possible military use.

As an addition to section 25.2 of the DPSS GTC 2025, upon delivery of [...*Description of product/service/software...*], the provider shall assume the following obligations arising from import certificates: [...*Further specify the obligations here...*].

B. Special provisions

27.2 Intellectual property rights to third-party products and pre-existing rights of the provider	WKV 1, possibly SLV 4 and HKV 3	<i>Alt, App</i>	<p>If third-party products and pre-existing rights of the provider are inseparable parts of a created work product, the DPSS GTC 2025 provide for a one-time licence for further use for the service procurer's own purposes as standard. In some cases, the service procurer may wish to freely reuse a specific work product, including independent further development and adaptation of the third-party product contained therein, as well as resale/sublicensing to a large number of its own customers. However, it is also possible that the provider cannot grant the standard licence in accordance with the DPSS GTC 2025 because of non-negotiable provisions with the third-party supplier and therefore wishes to amend the clause. However, such amendments are to be accepted only in exceptional cases and after a thorough examination of their compatibility with the purpose of the contract.</p>	<p><i>Differing provision to be used only in exceptional cases and only after an assessment of the case in question.</i></p> <p><i>In particular, it is important to ensure and check that the provider has the necessary rights from the third-party supplier or manufacturer to be able to make the adaptations to the licence for third-party products itself. In the event of an extensive transfer of rights or in case of uncertainty, the consent of the actual rights holder should be obtained as a precaution. This consent can also be included as an appendix and listed in the DPSS contract template under the existing heading "Appendices".</i></p>
28.7 Minor defects / and Significant defects 28.9 defects	WKV 1, possibly others	<i>Alt</i>	<p>It may be useful to define several classes of defects to enable better defect classification.</p>	<p>In deviation from sections 28.7 and 28.9 of the DPSS GTC 2025, defects shall be classified as follows:</p> <p><u>Error class A:</u> Serious errors that significantly restrict or prevent the use of [the complete system / the software / the</p>

hardware / the service] or parts thereof
(significant preventive defects);

Error class B: Errors that make it difficult to use [the complete system / the software / the hardware / the service] or parts thereof and that can be circumvented only with additional effort on the part of users (significant obstructive defects).

Error class C: Errors that make it difficult to use [the complete system / the software / the hardware / the service] or parts thereof but that can be circumvented with minimal effort on the part of users (minor defects).

29.2 Installation of purchased hardware

HKV 1

Alt

Under the DPSS GTC 2025, hardware installation is covered by the purchase contract as standard. Any differing provision must be agreed.

In deviation from section 29.2 of the DPSS GTC 2025, installation shall be carried out by the service procurer itself in accordance with the provider's installation instructions.

Alt 1

The parties agree that the roll-out and/or installation of the contractual hardware shall be covered by separate contracts.

32.4 Maintenance services for earlier software versions

WPV 5

Alt

The standard period during which the provider is obliged to maintain earlier software versions is limited to 12 months. This can be adjusted if necessary. Depending on the quote, a version support policy differentiated according to major and minor releases, patches, etc. may be agreed instead of the proposed clause. This centralised information source will indicate, among other things, how much notice the provider will give about the end of support for specific versions.

In deviation from section 28.4 of the DPSS GTC 2025, the period during which the provider is required to maintain earlier software versions shall be [...] months.