

GIBIT 2025

Explanatory notes to each article

VNG Realisatie
Nassaulaan 12
2514 JS Den Haag

www.gibit.nl

September 2026

Inhoud

I General provisions **4**
Article 1. Definitions 4
Article 2. Scope of Application 6
Article 3. Conclusion of the Agreement 8
Article 4. Performance of the Agreement 9
Article 5. Transport, Ownership and Risk of Products 10
Article 6. Implementation of ICT Deliverable 10
Article 7. Dependency on and Coordination with Third Parties 11
Article 8. Interoperability Requirements, Norms and Standards 12
Article 9. Acceptance 13
Article 10. Maintenance and Support 15
Article 11. Fees, Invoicing and Payment 18
Article 12. Warranties 21
Article 13. Algorithmic Applications 21
Article 14. AI Systems 22
Article 15. Documentation and Information 23
Article 16. Product Management 23
Article 17. Liability 23
Article 18. Insurance 25
Article 19. Confidentiality 25
Article 20. Force Majeure 26
Article 21. Intellectual Property 26
Article 22. Access to Data and Authorisations 27
Article 23. Third-Party Software 29
Article 24. Replacement of Personnel 30
Article 25. Software Bill of Materials 30
Article 26. Company Takeover 31
Article 27. Suspension, Termination and Dissolution 31
Article 28. Right of Inspection and Cooperation with Audits at the Client's Premises 33
Article 29. Exit plan, Transition, Limited Continuation, Transfer and Extended Use 33
Article 30. Applicable Law and Disputes 35

II Privacy,Security and Archiving **36**
Article 31. Data Processor Relationship 36
Article 32. Information Security 36
Article 33. Archiving 37

III Remote Services **38**
Article 34. General provision 38
Article 35. Acceptance Procedure 38
Article 36. Stored Data 39
Article 37. Maintenance and Availability 39
Article 38. Periodic Third-Party Statement 39
Article 39. Continuity Guarantees 39

IV Open Source **40**
Article 40. General Provision 40
Article 41. Delivery and Rights 40
Article 42. Repository 41
Article 43. Open Source License 41
Article 44. Management and Maintenance 42
Article 45. Additional Financial Arrangements 42
Article 46. Termination 42

I
General provisions

Article 1. Definitions

This article defines the various key terms used in the GIBIT. These terms are not explained individually, but are discussed in the various articles in which they are used.

In general, it may be noted that an effort has been made to keep the terms abstract and descriptive, and to exercise great restraint in incorporating substantive choices into them. The GIBIT terms and conditions remain generic and abstract in nature. After all, they must be applicable to a wide variety of situations.

In the GIBIT, the Supplier's counterparty is referred to as the 'Client'. This term was chosen because the GIBIT can be used not only by municipalities themselves, but also by municipal partnerships or other bodies (whether or not affiliated with the municipality). This is why, for example, the term 'Municipality' was not chosen. This explanatory note therefore consistently refers to the 'Client'. The choice of the word 'Client' is not, however, intended to define the legal relationship. Agreements concluded under the GIBIT may qualify as service provision agreements, sales agreements, mixed agreements containing a service provision element, or other types of agreements. It is entirely conceivable that the Agreement contains no service element whatsoever.

It should be noted that the following applies to all definitions: the mere fact that the Parties use different words in practice to refer to a concept (e.g. 'project plan' instead of 'implementation plan') does not affect the meaning, interpretation or legal consequences of that interpretation in the Terms and Conditions of Purchase.

The substantive changes to the terms in the GIBIT version 2025 compared to the 2023 version are as follows:

- Acceptance: A clearer distinction has been made between definitions and substantive requirements, as the requirements for Acceptance are separate from the meaning of Acceptance.
- Acceptance procedure: A clearer distinction has been made between definitions and substantive requirements, as the requirements for an Acceptance procedure are separate from the meaning of the Acceptance procedure.
- AI system: The term 'AI system' has been added. This is the same definition as that given to AI systems in the AI Act (Regulation (EU) 2024/1689), and should be interpreted in the same way.
- Algorithmic application: The definition of 'algorithmic application' has been expanded to clarify that AI systems are always algorithmic applications.
- Application landscape: This definition has been slightly amended in wording compared to the 2023 version, without any legal implications. The application landscape refers to the 'overall picture' of ICT within the Client's organisation. The Terms and Conditions of Purchase further refer to the 'relevant parts of the application landscape'.
- Tender Specifications: It has been clarified that the tender specifications comprise all documents provided as part of the tender process. These include documents which describe and explain, for example, the Client's organisation, the ICT Deliverable, the contractual and organisational

objectives, and the Client's intended use of the ICT Deliverable, as well as the tender procedure.

- Conversion: This definition has been slightly amended in wording compared to version 2023, without any legal implications. Sometimes, conversion will be necessary without fully replacing the existing system, or conversion from another system may be required. The GIBIT can now account for this as well. Furthermore, the definitions of Conversion and Migration have been separated, and a clearer distinction has been made between definitions and substantive requirements.

- CSIRT: The term CSIRT has been added. In the case of municipal authorities, this refers to the Information Security Service (Informatiebeveiligingsdienst: IBD) of the Association of Netherlands Municipalities (Vereniging Nederlandse Gemeenten: VNG).

- Data: The term 'Data' has been added. This is the same definition as that given to 'Data' in the Data Act (Regulation (EU) 2023/2854), and should be interpreted in the same way. This definition has been applied wherever the 2023 version used the term 'gegevens' when it should have been 'Data'.

- Documentation: This definition has been tightened up compared to the 2023 version. Documentation refers to technical and user documentation, such as manuals, and descriptions of the ICT Deliverable. It is important for the Parties to agree on which documentation is to be delivered and kept up to date. It is conceivable, for example, that the requirements for Documentation relating to Open Source software will be more extensive.

- Exit plan: The concept of an exit plan has been added. Although the term appeared frequently in the 2023 version, it had not yet been defined.

- Functional Recovery Time: This definition has been removed. Although the term was included as a definition in Article 1, it was not used elsewhere in the Terms and Conditions of Purchase. It has therefore been moved to the Terms and Conditions of Purchase (Article 10) and removed from the list of definitions.

- User Support: This definition was included in the text of the Terms and Conditions of Purchase in version 2023 (10.7) and has been moved to the definitions. It has also been clarified that User support relates solely to questions regarding the use of the ICT Deliverable; questions concerning, for example, a system to which it is linked are not covered by it.

- GIBIT 2025: The definition of GIBIT 2023 has been replaced by GIBIT 2025.

- Implementation: A clearer distinction has been made between definitions and substantive requirements, as the requirements for implementation are separate from the meaning of implementation.

- Terms and Conditions of Purchase: The definition of GIBIT 2023 has been replaced by GIBIT 2025.

- Annual Fee: This provision inadvertently omitted a provision for situations where the Agreement continues for longer than agreed. In such cases, the (actual) fee paid would be divided by the initially intended term. However, this would no longer be a realistic representation of an Annual Fee.

- Interface: This definition has been expanded. In the 2023 version, it only concerned interfaces between the ICT Deliverable and the Application Landscape, but it is also possible for an interface to be established with external systems. It is then up to the Parties to agree which interfaces are to be delivered and maintained.

- Licence: The term ‘right of use’ has been replaced by the term ‘licence’. This is a textual change without any legal implications.

- Customised Software: There was concern in the market that specific customisations to standard software (e.g. incorporating a municipal authority’s corporate identity) were also considered customised software. The definition has been refined to make it clear that cosmetic changes do not automatically transform standard software into customised software. There was also concern in the market that the distinction between Customised Software and Innovative Maintenance on request was not clear enough. This has been clarified. It has been made clear that the Parties must explicitly agree on the development of Customised Software. In that case, the Parties will also be able to make agreements regarding the (further) development of that Customised Software.

- Migration: The term ‘Migration’ has been separated from ‘Conversion’ and added.

- Client: In the 2023 version, the Client was referred to as the Party ‘for whose benefit’ the Agreement is concluded. However, the Agreement is concluded for the benefit of both Parties. A different definition is therefore more accurate.

- Open Source software: As Open Source is a new topic in the Terms and Conditions of Purchase, a definition has been drawn up for this.

- Party: In previous versions, the terms ‘party’ and ‘parties’ were used interchangeably, with and without a capital letter. For the sake of clarity, the term ‘Party’ is now capitalised throughout when referring to the Supplier and/or the Client.

- Software: It has been added to the definition of Software that this also includes the Interfaces to be supplied.

- Response time: This definition has been removed. Although the term was included as a definition in Article 1, it was not used elsewhere in the Terms and Conditions of Purchase. It has therefore been moved to the Terms and Conditions of Purchase (Article 10) and removed from the list of definitions.

- Service Levels: Although the terms ‘functional recovery time’ and ‘response time’ were included as definitions in Article 1, they were not used elsewhere in the Terms and Conditions of Purchase. It has, therefore, been moved to the Terms and Conditions of Purchase (Article 10) and removed from the list of definitions.

- Upgrade: There was concern in the market that the distinction between Customised Software and Innovative Maintenance on request was not clear enough. This has now been clarified. It should be noted that it is up to the Parties to reach clear agreements regarding further development under contract versus the development of Customised software. The aim is for municipalities and suppliers to coordinate this in a strategic manner, for example through user associations that draw up the roadmap for new functionalities.

- Fee: The previous definition was still based on a term, whereas the definition of ‘annual fee’ was created specifically for this purpose.

Article 2. Scope of Application

This article sets out some general provisions regarding the scope of application of the GIBIT. In this context, ‘ICT Deliverables refers to the total scope of Products, services and Licences to be supplied.

Article 2.1 stipulates that the GIBIT applies not only to the ICT Deliverables under the Agreement, but also to related ICT Deliverables – which may be agreed upon in the future. The aim is to prevent a different set of terms and conditions suddenly applying to subsequent, additional agreements. Naturally, deviations from this are possible; the terms and conditions serve as a safety net.

Please note: there is no intention to bind Suppliers to the GIBIT in advance for all future contracts The provision applies only to agreements that are related to an agreement in which the applicability of the GIBIT has already been stipulated. An example is where a maintenance agreement is subsequently concluded at a later date, even though it was not originally part of the Contract. This maintenance agreement will then be subject to the terms and conditions of the GIBIT. Clients should therefore be aware that, prior to concluding an agreement – i.e. as early as the quotation request/tender stage – they must declare the GIBIT to be applicable. This ensures that the GIBIT applies as terms and conditions from the outset, including for additional Agreements concluded at a later date.

The safety net nature of the GIBIT also means that irrelevant provisions do not necessarily have to be deleted For example, if the Agreement does not concern Products, the provisions relating to Products may simply remain in place; they will simply not apply. This facilitates the conclusion of Agreements; there is no need for customisation in this regard.

Article 2.2 concerns the division of the GIBIT into four chapters. The general Chapter I always applies; the other chapters, containing provisions on privacy, security, archiving, Remote Services and Open-Source Software, apply depending on the nature of the Products/services to be supplied (supplementary).

Article 2.3 has been included to exclude the general terms and conditions of Suppliers, even where reference is made to them at a later date. The purpose of this provision is to ensure that the GIBIT remains applicable in the event that Suppliers declare their own terms and conditions to be applicable. The provision is linked to the provisions of Article 6:225(3) of the Dutch Civil Code (Burgerlijk Wetboek). This states, in essence, that the general terms and conditions declared applicable first, shall remain applicable, unless, upon declaring a second set of general terms and conditions applicable, the first set has been expressly rejected. It is, however, open to question whether the provisions of this article meets the requirement of express rejection as referred to in Article 6:225(3) of the Dutch Civil Code. Clients should therefore always be vigilant to ensure that Suppliers do not declare their own terms and conditions applicable in the offer.

Article 2.4 has been included to ensure that, should any provision of the GIBIT be invalid:
1. this will not affect the validity of the other provisions of the GIBIT; and
2. the Parties will be required to enter into new agreements that take the purpose and intent of the original provision into account.

Article 2.5 stipulates that the Agreement takes precedence over the provisions set out in the GIBIT, whilst the further Agreement and any terms and conditions relating to Third-Party Software and Open Source Software, in turn, take precedence over these documents. This is a very important provision. This is due to the abstract nature of the GIBIT and the fact that the GIBIT serves as a safety net. For the record: the Agreement between the Client and the Supplier may deviate from any provision in the GIBIT. The fact that some provisions in the GIBIT expressly refer to the Agreement and others do not is irrelevant in this regard. References to the Agreement have, where applicable, been included solely to draw additional attention to the possibility of deviation.

The paragraph also stipulates that the terms and conditions of Third-Party Software, provided they have been duly declared applicable, prevail over the agreements between the parties. The rationale behind this is that a third party may implement updates, refuse warranties, etc., without the supplier having any influence over this. This does not refer to licence and maintenance terms and conditions in the literal sense, but in a broader sense. The terms and conditions of sale and warranty of that supplier are also included. Incidentally, this applies only to software, not to hardware. Article 2.6 stipulates that the law applies as a safety net. Contract law consists, in essence, almost entirely of non-mandatory law. The law thus provides the ‘default’ position, unless the Parties agree otherwise. In legal practice, however, opinions differ as to what the existence of a contract means for those aspects of the non-mandatory law where the Parties have not made an explicit choice: does the aforementioned ‘default’ remain in force, or does only the contract apply?

To put an end to this uncertainty, the Terms and Conditions of Purchase stipulate that the non-mandatory law remains applicable in principle.

Finally, Article 2.7 stipulates that any amendments to the GIBIT must be agreed in writing. It also stipulates that such amendments apply only to the Agreement referred to in Article 2.1. This is based on the principle that, for each project, it must be reassessed which provisions are relevant and which are not.

Article 3. Conclusion of the Agreement

This article clearly sets out the Supplier's duty of care. This duty of care for Suppliers applies in any event by virtue of the law and case law (see Article 7:17(5) of the Dutch Civil Code regarding sales, Article 7:401 of the Dutch Civil Code regarding service provision contracts, Article 6:228 of the Dutch Civil Code regarding the duties to disclose information under, etc.). However, it is often unclear what exactly is meant by this abstract duty of care. That is why it is further defined here in Article 3.

As will be explained in more detail below, the GIBIT seeks to strike a balanced approach to the interests of the Parties through the provisions on risk analysis. These provisions prevent the Parties from having to rely on concepts that are not clearly defined, such as 'duties of care', and instead provide a clear framework based on a risk that is, in principle, foreseeable.
The GIBIT further specifies the duty of care with regard to the pre-contractual phase. The Supplier must not only familiarise himself thoroughly with relevant information about the Client and the proposed project (articles 3.2/3.3), but must also act upon this by incorporating this information into the quotation and the risk analysis (articles 3.4/3.5). In effect, the Supplier is expected to comply with the 'know your customer' and 'know your product' principles. Furthermore, as the Supplier must warn the Client of any risks identified, this ensures that the Client is aware in advance of the risks that must be taken into account. If the Client has explicitly stated in his request for proposals what must be submitted with the tender, the Supplier cannot be expected to provide much more than that, unless he has reasons to 'protect the Client from himself'.

The rationale is that this will bring the risk assessment forward in time, ensuring both Parties have a clearer understanding of the commitment and can implement timely mitigation measures.
The nature and scope of the risk analysis will vary from one assignment to another. For small assignments or projects, it is conceivable that the assessment will be minimal and, so to speak, limited to the Supplier explicitly pointing out the system requirements and enquiring about the use of any incompatible combinations of hardware and software known to the Supplier; for large assignments and projects, more will be required of both Parties. On-site research at the Client's premises is not strictly necessary. A Supplier who is familiar with his own Product and has experience in implementing it knows what information is required to be able to make a sound offer and which pitfalls in that offer need to be addressed (or at least ought to know this).

In highly risky and complex projects, it is advisable to obtain separate advice on the risks, either from the Supplier himself as a separate (sub-)assignment or from a third party.
It must always be borne in mind that the risk analysis is part of the pre-contractual duty of care. This analysis therefore does not go beyond what may reasonably be expected of a Supplier prior to the contract. It is precisely a Supplier who knows his own Product who can, where appropriate, give timely warning (and also explain clearly) that a proper risk analysis requires so much time and effort that, in that specific case, it is not reasonable to regard this as part of the quotation phase.

It should also be emphasised that the Client is obliged to cooperate with the risk analysis by providing any information reasonably requested (Article 3.3), such as a description of the Application Landscape. Should the Client fail to do so, he will be in (creditor's) default in respect of that obligation. Incidentally, this would also have been the case even without explicit wording in

the GIBIT. In the event of such a lack of cooperation on the part of the Client, the Supplier cannot be expected to do more than submit its quotation on the basis of the information that is available. Suppliers would therefore be well advised to document, and preferably specify, the information on

which their quotation is based. This makes it clear to both Parties what the basis for the collaboration is. The most significant consequence of a breach of the aforementioned 'know your customer' and 'know your product' principles is that the Client may claim compensation for adjustments to its own IT environment that were necessary during the Implementation but were not disclosed in advance.

In theory, a Client could also terminate the Agreement as soon as it becomes apparent that the Supplier has failed to make an appropriate offer. However, precisely because the GIBIT already contains the solution described above for that situation, aimed at the progress of the project, and because Clients must always observe reasonableness and fairness when exercising their powers, termination is not the obvious course of action in that situation. This makes the provision in the GIBIT nuanced and certainly not solely in the interests of Clients.
Information and transparency regarding Third-Party Software are essential, including in the pre-contractual phase. That is why paragraph 5 includes various information obligations relating to Third-Party Software. The thinking behind this is that the Client can thus make an informed decision as to whether or not to accept the use of that Third-Party Software and the associated terms and conditions. After all, those terms and conditions take precedence over what is stipulated elsewhere in the Agreement (Article 2.5).

Under sub-paragraph (iv), the Supplier must also specify in the tender any dependency on third-party software. Experience shows that, in discussions regarding performance, for example, third-party software is (too) quickly cited as the cause. By being informed of such dependencies in advance, the Client can also make an informed decision on this point. Furthermore, this prevents the improper use of this argument.

Depending on the value of the contract and/or the Clients' own policies, a contract may be put out to tender. Public procurement legislation restricts the scope for Suppliers to make enquiries directly with Clients during the tendering process. This is acknowledged in Article 3.6 of the GIBIT.

The term *'in writing'* in Article 3.7 refers to *'written*', not *'on paper'*. Electronic communication is therefore also permitted.

Article 4. Performance of the Agreement

GIBIT's basic principle is that deadlines are not strict, except for:
a. agreed completion dates for the primary Implementation; and
b. agreed dates for the Implementation or delivery of Updates/Upgrades in connection with the entry into force of changes to legislation and regulations.

This is in line with the structure of the law. It is important that dates for Implementation are strict deadlines; often, the Go Live date of an IT Deliverable will be linked to the phasing out of an old system. This article should also be read in this light. If aftercare is also considered part of the Implementation, this aftercare phase should not be included when determining the strict deadline.

Furthermore, the effective date of (changes to) legislation and regulations is also set as a strict deadline. This is only different if such laws and regulations were not foreseeable or if the period before their entry into force was demonstrably too short. This is unlikely to be the case. This may include, for example, emergency legislation or regulations that come into force immediately.

Article 4.4 allows for the risk analysis referred to in Article 3 to be carried out at a later stage, for example during the proof-of-concept (POC) phase or the verification phase. This allows Suppliers to avoid having to invest a great deal of effort in the risk analysis as early as the quotation phase. The risk that unacceptable risks may emerge at this later stage is covered by the Client's right to terminate the Agreement in such a situation (subject to reimbursement of costs incurred).

Suppliers do not have this right. This was a deliberate choice: after all, a Supplier may be expected to have a clear understanding of the risks on their part regarding the delivery of the ICT Deliverable as early as the initial quotation (before the risk analysis has been carried out). This is also why it is

explicitly stated that the Supplier must identify generally known risks at the time of the quotation.

Article 4.5 expressly stipulates that the Client shall comply with all obligations arising from the Agreement. Strictly speaking, this provision is superfluous, as this is already stipulated in the law and the Agreement. The provision primarily serves as an important signal, both to Clients and to Suppliers. It is important for Clients to fully realise that the agreements made – for example, in the Implementation Plan – regarding the work to be carried out, must also be fulfilled (in a timely manner).

For the sake of completeness, we would point out that, in the event of a breach of this duty to cooperate, Suppliers may invoke suspension (including retrospectively). In this case, the Client will be in creditor's default and the Supplier can (therefore) no longer be in default himself. Adequate cooperation on the part of the Client is therefore of crucial importance. However, given the statutory duty of care incumbent on Suppliers, it is likely that Suppliers may be expected to urge the Client, where necessary and in a timely manner, to fulfil his (cooperation) obligations.

Article 5. Transport, Ownership and Risk of Products

Article 5 consists largely of procedural arrangements that are self-explanatory; its content is largely taken from Articles 6 and 7 of the ARBIT.

Article 5.6 deliberately departs from the ARBIT: whereas the ARBIT assumes that a transfer of ownership has taken place, the GIBIT merely sets out preconditions for cases where a transfer of ownership has been agreed. This is because, in practice, Products are increasingly not being sold but are being made available under a different title

Article 6. Implementation of ICT Deliverable

GIBIT assumes that the Supplier will be responsible for the Implementation. The term 'Implementation' is deliberately defined broadly (see Article 1) and refers to the controlled, project-based deployment and commissioning of the ICT Deliverable within the organisation, as well as its integration into the existing information systems. The latter, of course, must be carried out within the framework of the Agreed Use. The Implementation therefore does not lead to any changes to the agreements made regarding the functionality to be delivered. Naturally, the obligations regarding Implementation do not apply if the ICT Deliverable is not implemented or cannot be implemented.

In this context – in the abstract – it makes no difference whether the service being implemented is an on-premise or a SaaS service. After all, in both cases, steps will need to be taken – to a greater or lesser extent – to ensure that the IT Deliverable can be put into operation. The nature of the implementation work will, of course, differ.

Article 6 addresses the early identification of risks. Article 6.1 stipulates that the Implementation shall take place in accordance with the Implementation Plan, and Article 6.2 sets out the elements to be included therein. Article 6.3 specifies the preconditions for the Conversion and Migration during the Implementation. In this regard, Data must remain intact and be transferred exactly as is (one to one). In principle, the same applies to metadata (a structured description of the content or use of data that facilitates the discovery and use of that data), but this will not be possible in exceptional cases. After all, when migrating to a new system, different metadata structures are often used. However, the Supplier shall ensure that metadata is transferred (demonstrably) as intact as possible.

Article 6.4 further stipulates that the drawing up of such a plan may always be required, and that, in principle, it must be delivered within three months. Naturally, the Supplier cannot be expected to draw up a plan within three months if one of the other parties involved is obstructing the process. Article 6.5 also specifies which topics must be included in such a plan. The idea is that it is in the interests of both Parties to give careful consideration in advance – and not only as the project progresses – to everything necessary to ensure the success of the Implementation. Incidentally, in practice, not all the topics listed in Article 6.5 will be relevant to every project. For this reason, 'where applicable' is included in brackets.

Article 6.6 sets out provisions regarding the involvement of third parties in end-to-end testing and specifies that the provisions on the timely involvement of third parties apply mutatis mutandis to the entire Implementation.
New in the 2025 version is Article 6.7. In practice, it is sometimes the case that licences are already being offered whilst a (long) Implementation is still ongoing. In such a situation, a Client is already paying for everything, whilst not yet deriving any benefit from it. It is therefore the Supplier's duty to offer only those Licences that are necessary for the Implementation, such as test licences. It is conceivable that certain licences fall into a grey area: they are not strictly necessary, but they are useful. Even with these licences, the Supplier cannot unilaterally impose an obligation to purchase them. The parties will need to discuss this.
Article 6.8 refers to the risk analysis referred to in Articles 3 and 4. It stipulates that any adjustments to the Client's application landscape that are necessary but were not foreseen in advance, yet which, in view of the Supplier's duty of care, could have been foreseen retrospectively, shall be borne by the Supplier. In this respect, the article constitutes the 'proof of the pudding' regarding (the quality of) the aforementioned risk analysis concerning the compatibility of the proposed solution for the Client. The article only applies to modifications to the Application Landscape that the Supplier could or ought to have foreseen. The article seeks to prevent Suppliers from knowingly submitting an incomplete or poorly considered proposal during the award process in order to gain an advantage and later being 'rewarded' with additional work orders.

Furthermore, this article only applies to modifications to the Application Landscape that are necessary for the Implementation (and therefore for the Agreed Use). The article therefore certainly does not constitute a free pass for Clients to have all kinds of components of the Application Landscape, unrelated to the Implementation, upgraded at the expense of Suppliers, or to demand improvements that go beyond what is necessary for the Implementation. For more extensive modifications, the Client must enter into new/separate agreements. If, in practice, it becomes apparent that it is advantageous for the Clients to go beyond what is strictly necessary for the Agreement when making modifications to the Application Landscape, it stands to reason that the Parties should enter into separate agreements in this regard (e.g. a separate Upgrade project with a discount).

Article 6.9 concerns the Supplier's willingness to subsequently or once again perform activities related to the Implementation. Examples include a Conversion to be carried out after commissioning or going live, the creation of additional Interfaces after going live, or the provision of (additional) training after going live. In the case of tendered contracts, it is important to assess whether such an additional assignment does not result in a substantial change to the contract

Article 7. Dependency on and Coordination with Third Parties

Article 7 sets out in greater detail the existing provisions regarding dependency on third parties. The article concerns reliance on third parties who are not an auxiliary person of either Party (Article 7.1). After all, the Parties are themselves responsible for the auxiliary persons they engage. This article specifically concerns third parties that are independent of the Parties, such as suppliers of other ICT Deliverable that must be connected to the ICT Deliverable in question, or owners of buildings where equipment is to be installed (to mention two very different examples).

Article 7.2 sets out which Party is generally responsible for determining and notifying the other Party ('raising the alarm') if such a dependency exists. This is nothing more than a duty to notify. The rationale is that, in the case of Remote Services, it is the Supplier who is particularly well placed to know whether such a dependency exists, whereas for other services it is more obvious to assign this task to the Client, as the Client will (or ought to) be the best acquainted with his own application landscape. The latter does not affect the Supplier's duty to identify risks in the initial proposal (see Article 3.4). The Parties must also – needless to say – draw each other's attention to risks of which they are already aware or ought to be aware, even if these fall within the other Party's sphere of responsibility. It must be avoided that the Parties rely blindly on the information provided by the other party.

Article 7.3 stipulates that further agreements must be reached on a number of specified matters. The main purpose of this provision is to ensure that such agreements are reached as early as possible and to avoid any surprises later on. In this context, see also Article 7.5: the basic principle here is that the third party should also be involved in the consultations at an early stage and that agreements should be reached with them in advance as well.

Article 7.6 contains a nuanced arrangement on how to deal with blocking issues that are not attributable to the Supplier but to a third party. Essentially, this article concerns (i) a duty to consult should an issue arise whereby the ICT Deliverable does not function as agreed, whilst the cause of this does not lie with the Supplier (but with third parties, or with the Client himself) and (ii) the recognition that, in such a situation, the Supplier is simply entitled to what has been agreed regarding the consequences of Acceptance (in practice, this usually means payment).

Article 8. Interoperability Requirements, Norms and Standards

One of the GIBIT's objectives is to improve the quality of the information provided by municipalities and of the ICT products and the services that form part of this. The GIBIT also wishes to promote standardised data exchange so that information can be shared effectively, securely and reliably, and processes can be carried out in a chain-oriented manner. This is reflected in Article 8.

Article 8 stipulates that the ICT Deliverable must comply with all prescribed standards. The Municipal ICT Quality Standards (Gemeentelijke ICT-kwaliteitsnormen) (the document setting out mandatory standards) play a central role in this regard: parties are encouraged to declare these standards applicable and to work in accordance with them. A new feature of the 2025 version is that the standards no longer always apply, but only if the parties choose to do so. In order to prevent standards from conflicting, particularly where core obligations are concerned, it is essential to specify them explicitly. It would be contrary to the principle of transparency to impose core obligations such as these via a single reference in general terms and conditions of purchase.

Also new is the possibility to use, instead of the Municipal ICT quality standards, comparable and recognised standards as a benchmark. Examples of such standards include ISO/ISAE/NEN standards. After all, the aim of the provision is not merely to promote the Municipal ICT Quality Standards, but to ensure a high level of security. If that level can be guaranteed without the Municipal ICT Quality Standards, then that is also acceptable and proportionate. The Supplier will have to demonstrate that the standards are comparable and widely accepted internationally.

In the Municipal ICT Quality Standards, VNG Realisatie specifies which standards apply to certain types of applications or ICT products/services. It is possible to declare all Municipal ICT Quality Standards applicable, but it is advisable to specify the standards to be implemented in the tender and to discuss them with the Supplier. At that point, it is also possible to consider whether an alternative standard would be sufficient. This certainly applies where the (correct) implementation of a standard is important for the success of a procurement process. Both Clients – who are thus compelled to consider (the importance of) standards for a specific project – and Suppliers – who are specifically made aware of their importance – stand to benefit from this.

The Municipal ICT Quality Standards are published periodically by VNG/VNG Realisatie. The set includes only those standards and specifications that are mandatory within the scope of application of municipalities, municipal partnerships or the chains in which municipalities operate. These are open standards and specifications in the development of which suppliers have been involved.

When determining which norms and standards are relevant and may be prescribed, reference can be made to the list of open standards as established and published by the Secretariat of the Netherlands Standardisation Forum (bureau Forum Standaardisatie) (also known as the commonly used standards and/or standards on the 'comply-or-explain' -explain list (pas-toe-of-leg-uit lijst)) and standards that have been established as national or municipal standards by VNG/VNG Realisatie. These are norms and standards covering the following ICT quality areas (for clarification purposes, examples of relevant norms and standards are given in brackets, with subsequent versions also falling under these standards):

- Architecture (GEMMA);
- Interoperability (NEN3610, Stuf, SUWIML, Digikoppeling, iWMO);
- Security (Municipal Information Security Baseline);
- Data portability;
- Meta data management (TMLO);
- Accessibility (Web Guidelines);
- Archiving (NEN-ISO 15489-1 NL, NEN-ISO 16175-1);
- Infrastructure (Generic Digital Infrastructure, connection to the System of Basic Registries);
- Documentation;
- E-invoicing.

Many standards and regulations require that certain preventive tests be carried out in order to demonstrate compliance with the relevant standard. Article 8.2 stipulates that these tests must be carried out prior to Implementation. Article 8.2 also stipulates that the Supplier must submit this test report to the Client, so that both Parties have access to the same information.

Whereas the 2023 version assumed testing would take place in a non-production environment, that requirement has now been dropped. Practical experience has shown that this is by no means always necessary and/or proportionate. However, if the Client requests to do so in certain circumstances, the Supplier will still provide this environment If this request has already been specified in the Tender Specifications, it forms part of the agreement. If this is a request made at a later stage, it is only logical that the Client should pay for this.

Incidentally, the municipality cannot expect an alternative environment to function exactly the same as the real environment. Printing, emailing and links to other applications will have their own limitations.

Under Article 8.4, repeat preventive testing is unnecessary if the tests have already been successfully completed under comparable conditions using the same version of the Product, the standard and the test set. This means that the article on preventive testing is relevant particularly in the case of new Products, new versions of Products or Products that have not yet been used in a comparable context.

Incidentally, an additional test is not mandatory if the Supplier can demonstrate that it has already carried out such tests. After all, it cannot be expected of the Supplier to keep testing Standard Software indefinitely. However, this may be different if it is demonstrated that an additional test provides greater certainty.

Article 8.6 states (for the sake of completeness) that during the Acceptance Procedure, an assessment is made of the extent to which the IT Deliverable meets the standards. Strictly speaking, this already follows from the fact that compliance with the standards forms part of the 'Agreed Use'.

Article 9. Acceptance

Article 9 sets out the Acceptance Procedure. This is defined in Article 9.1. It is in the interests of both Parties that it is clear, in advance, how the acceptance procedure will be conducted. This is why Article 6.4 sub-paragraph(ix) stipulates that, as part of the Implementation Plan, the manner in which the Acceptance Procedure is to be carried out must be specified. However, there will not always be an Implementation Plan. It is also conceivable that the Implementation Plan contains no, or insufficiently detailed, agreements regarding the Acceptance Procedure. Hence, Article 9.2 stipulates that, at the Client's request, a written test protocol shall be drawn up. The reference to Article 6.3 is intended to indicate that the Supplier is the lead drafter of the plan (as the most expert party) and may not charge a separate Fee for drawing up the plan.

The remaining provisions of Article 9 should be regarded as 'safety-net provisions'. These provisions provide the framework insofar as no more specific arrangements regarding the Acceptance Procedure have been made in the Agreement or in any other higher-level document. All of these provisions together describe the Acceptance Procedure.

Article 9.3 essentially sets out what takes place during testing. We will explain the elements point by point:

- Testing is carried out for Defects, i.e. failure to comply with the Agreed Use. Tests are expressly not carried out on aspects of the ICT Deliverable that have not been agreed upon (as this would not be attributable to the Supplier). Testing is, however, carried out on the concept of Agreed Use, which is broader than merely what is set out in the terms of reference (partly due to the duty of care set out in Article 3);
- The results of the Acceptance Procedure shall be recorded in writing in a test report. This report shall be signed by the Parties. The idea is that this will minimise any discussion afterwards regarding the outcomes of the Acceptance Procedure;
- The Supplier must provide a schedule for the rectification of any Defects identified. In accordance with Article 9.4, this schedule must fit within the overall project schedule;
- Following the rectification of the Defects, the Supplier shall resubmit the ICT Deliverable for Acceptance. An Acceptance Procedure shall then, once again, follow in accordance with the principles described above.

Article 9.4 has already been briefly mentioned. The article stipulates that the rectification of Defects identified during testing must not lead to any delay. It is therefore up to the Supplier – partly in view of its role as the lead drafter of the offer (Article 3), the Implementation Plan (Article 6) and/or the test protocol (Article 9.2) – to adopt a realistic schedule in advance, allowing sufficient time for the rectification of any Defects identified. It is, moreover, part of the Supplier's duty of care to monitor the progress of the Implementation and, where necessary, to warn the Client or even to demand action. This demand notice must be issued within 5 working days. This duty of care is based on existing case law (see inter alia ECLI:NL:GHSHE:2015:4428, paragraph. 3.8.4). Should a Client fail to respond adequately to this, the ball will be in his court (Article 9.5). A deadline may, for example, be suspended as a result.

Article 9.6 states that the aforementioned nuanced provision regarding dependency on third parties applies mutatis mutandis.

Article 9.7 stipulates that any Interfaces with other systems must be tested for proper interoperability during the acceptance procedure. After all, many applications only function properly in the context of integrations with other applications. Whilst this is often not readily apparent to the end user, it is essential for secure and reliable information chains.

Article 9.8 sets out the various scenarios in the event that the Acceptance Procedure is unsuccessful:

1. termination of the Agreement; or
2. rectification of the Defects at no cost; or
3. acceptance subject to a further condition, on the understanding that if the condition is not met, the Agreement may still be terminated with immediate effect.

These three options give Clients considerable flexibility in how to deal with any Defects:

1. if key aspects of the IT Deliverable are not up to standard, termination is the obvious course of action;
2. in the case of minor Defects, rectification at no cost is the obvious course of action; and
3. in the event of late delivery of parts of the Service that will only become relevant to the Client in the future, conditional Acceptance is the obvious course of action (namely Acceptance on the condition that the ICT Deliverable has been correctly implemented by the date on which the currently missing parts become relevant to the Client).

The GIBIT has deliberately opted to allow for immediate termination after two rounds of testing, without the need for a further notice of default The thinking is that, in principle, two opportunities to deliver the agreed performance should be sufficient. Furthermore, this encourages thorough and careful testing.

It should be noted that, in an Acceptance Procedure, the Client is required both to provide all necessary cooperation with the Acceptance Procedure and to fulfil his own obligations (as set out in the Implementation Plan and/or test protocol). If the Client fails to do so, the Supplier may invoke suspension and the Client will be in creditor's default. See also the explanatory notes to Article 4.5. If the Client is in creditor's default, he will of course not be entitled to termination. The latter follows from the law and the GIBIT (deliberately) does not deviate from this.

Article 9.9 stipulates that the contract may not be terminated on the grounds of defects that are first identified in the second round of testing, while these could also have been identified earlier in the Acceptance procedure. This forces clients to take the acceptance procedure seriously and give it the attention it deserves.

Article 9.10 allows the Parties to agree, if necessary, that certain defects may be remedied outside the existing schedule.

Article 9.11 expressly stipulates that Defects which do not prevent the project from being put into operational use, cannot constitute grounds for non-Acceptance. The rationale behind this provision is that a project should not be rejected on a formality, but only on the basis of Defects that are actually relevant or material to the Client. This does not, however, affect the obligation to remedy even those less relevant Defects. After all, the delivery of the functionality in question has been agreed.

Article 9.12 stipulates that, where partial deliveries have taken place, a full Acceptance Procedure must also be carried out following the final partial delivery. This expressly acknowledges that, in the case of ICT Deliverable, the individual parts may function correctly (insofar as they can be assessed as separate components), but the sum of the parts may not, whilst the Client is naturally concerned with the sum of the parts (the total ICT Deliverable).

Finally, Article 9.13 establishes a presumption of Acceptance if the ICT Deliverable has been put into use for operational purposes, unless such early use is attributable to delays or failures on the part of the Supplier. It is conceivable that, in the event of a delayed delivery, a Client may be compelled to take the ICT Deliverable into use (e.g. because otherwise there is no in-house ICT to support a new law), but that does not imply that the Client has (therefore) also accepted the ICT Deliverable. However, if the Client deliberately chooses in advance not to conduct an Acceptance Procedure and subsequently puts the ICT Deliverable into use for operational purposes, it thereby implicitly accepts that the ICT Deliverable may still contain Defects upon delivery, which will then be (or can/must be) addressed within the framework of Maintenance (Article 10).

Article 10. Maintenance and Support

The starting point of the GIBIT is that the maintenance phase follows Acceptance. The GIBIT provides an (abstract) framework for the maintenance phase. In practice, this framework is usually set out in more detail in the Agreement or in a separate maintenance agreement/SLA.

Given the importance of ICT systems continuing to function properly, a conscious decision has been made to provide, as a standard arrangement, that the Supplier shall perform the Maintenance (Article 10.1) and that this Maintenance, by default, includes all forms of Maintenance referred to in Article 10.3. Of course, it is also possible for the Agreement to stipulate that the Supplier does not perform Maintenance, or only performs some of the forms of Maintenance listed in Article 10.3.

Article 10.2 once again emphasises the 'safety net' nature of the GIBIT. The provisions of the GIBIT serve as a basis, but the Agreement or SLA may deviate from them. The GIBIT contains few specific standards regarding Maintenance, apart from a few abstract requirements (which are discussed below). The specific standards (Service Levels) to be complied with by the Supplier will therefore need to be included in the Agreement or SLA. Furthermore, various practical aspects relating to the provision of Maintenance will need to be further defined (such as how and where a Defect must be reported). In many cases, such a maintenance agreement or SLA is, therefore, necessary.

Article 10.4 sets out the principle that Maintenance must cause as little disruption as possible to the Client's operational processes. A conscious decision has been made not to specify the exact times at which Maintenance may or may not take place, as this depends too heavily on the precise nature of the ICT Deliverable and the processes in which it is used. After all, coordination is not always easily achievable when Maintenance is carried out in bulk.

The primary consideration with regard to Maintenance must be that the Client does not experience any reduction in functionality (paragraph 5).

Article 10.6 stipulates that the Supplier must, in any event, be reachable on working days between 09:00 and 17:00. The term 'reachable' has been deliberately chosen, without specifying which channel or means of communication must be used. This leaves Suppliers sufficient scope to organise this themselves (telephone, email, chat, etc.). A certain degree of reciprocity has also been introduced: the municipal authority must also be available for Maintenance. This reciprocity is less strict than the obligations incumbent on the Supplier, as municipal authorities cannot always guarantee that someone with the necessary expertise will be available to respond immediately. What is possible, and is recognized in this paragraph, is that municipalities must, at a minimum, be available to consult with the Supplier during business hours.

For maintenance work to be carried out effectively, it is sometimes essential that the Client is also available, for example for coordination, testing or communication during the maintenance work. The requirement for the Client to be available for this purpose is set out in paragraph 7.

Article 10.8 states that all malfunctions may be reported, including non-attributable malfunctions.

Article 10.9 elaborates on the principle described above: all malfunctions (in the broadest sense) may be reported. If the reported issue does not constitute a breach, the Parties may consult on any additional work to be carried out as extra work. Examples of this include a situation where an employee of the Client has altered important settings in the ICT Deliverable contrary to the Supplier's instructions, or where a virus outbreak, not attributable to the Supplier, necessitates various repair works. For the sake of completeness, it should be noted that this concerns an attempt at repair (since this is a situation not attributable to the Supplier).

Article 10.10 relates to the 'safety net' nature of the GIBIT. It stipulates that the Supplier must be willing to enter into a further SLA. A specific requirement for this SLA is that Service Levels may be included therein, and that failure to meet those Service Levels will result in measures being taken. The nature of those measures will need to be determined on a case-by-case basis. It is important for the Client that the measure provides sufficient incentive for the Supplier to comply and, moreover, yields something that is also of benefit to the Client. As no model SLA can be provided, version 2025 specifies at least two key KPIs that must be included as Service Levels: response time and functional recovery time. This is because it is important that the Supplier provides clarity on these two points, at the very least. These are, therefore, obligations of result (resultaatsverbintenissen).

Articles 10.11, 10.12 and 10.13 stipulate that termination of the Agreement(s) is in any event possible in case of repeated failure to meet the Service Levels. This provision has been included to avoid the debate as to whether failure to meet a Service Level always constitutes a breach and/or the debate as to whether such failures always justify termination of the Agreement. Furthermore, it is stipulated that the measures set out herein, shall not affect the other rights of the Clients. This is to prevent a penalty stipulated in the SLA from being deemed, under the law, to constitute a fixed compensation (Article 6:92(2) of the Dutch Civil Code).

Compared to the 2023 version, the escalation ladder between the Parties has been expanded. If the Supplier fails to meet the Service Levels, the Client's options are normally to terminate the contract or to accept the breach of contract. In practice, both of these options are often undesirable. The previous version, therefore, already provided that an improvement plan and/or a management meeting could serve as intermediate steps before proceeding to termination. A new feature is the

option to agree on a penalty scheme as part of the improvement plan, to prevent further escalation. This may include, for example, the forfeiting of service credits or the incurrence of fines. Service credits are a form of compensation that a Supplier may pay to a client if the supplier fails to meet the agreed performance levels in the SLA. This may, for example, consist of a percentage of the monthly fees, or another form of crediting.

When determining the amount of the penalty, the EMVI penalty may be taken into account. Failure to meet Service Levels is really problematic from a procurement law perspective: if other tenderers could have been able to sufficiently meet these requirements, the contract may have been awarded to the wrong party.

Article 10.14 sets out a number of requirements regarding Preventive Maintenance. It is of the utmost importance to Clients that legislation and regulations are complied with at all times and that interoperability is maintained. Security advisories issued by the NCSC, its legal successor or otherwise made public must also be followed as soon as possible, and risks must be mitigated as soon as possible. The manner in which this is done is expressly at the discretion of the Supplier (see also the words 'or otherwise'). However, the paramount consideration is that (the use of) the ICT Deliverable must be safe, which certainly does not appear to be an unreasonable requirement.

This is a demanding requirement for Suppliers, but an important one for Clients. After all, virtually all municipal products, services, processes and information chains are, in one way or another, linked to compliance with legislation and regulations. As a result of increasing digitalisation, this has an impact on the quality requirements for ICT products and services. The GIBIT therefore assumes that the Supplier, as a specialist provider of specific software designed to support certain legislation, is (or should be) far better placed than the Client to translate changes in legislation in a timely manner into the necessary (technical) adjustments to the ICT Deliverable. For the sake of completeness, it is also stipulated that the obligation relates to the legislation and regulations relevant to the Agreed Use (and therefore not all conceivable legislation). The costs for such adjustments are, in principle, included in the maintenance fee. Please note: Supporting entirely new legislation generally does not fall under the 'Agreed Use' (and thus Maintenance) and is therefore not covered by the obligation under this article. This is laid down in article 11.3; see also the explanatory notes there.

Article 10.15 sets out the framework for the installation of Updates and Upgrades. The basic principle is that the Client is, in principle, responsible for installing Updates and Upgrades itself. The article does, however, stipulate that the Supplier may do so upon request (and for a fee). In that case, the provisions regarding Implementation and Acceptance shall also apply.

Article 10.16 seeks to establish a nuanced arrangement regarding the refusal of the installation of new Updates or Upgrades. On the one hand, the Client has the right to refuse such installation; on the other hand, the Supplier's obligations in the context of Maintenance are somewhat mitigated if the Client decides not to install offered Updates or Upgrades (immediately). In this case, the Supplier is only obliged to continue providing User Support (except for Defects that have not yet been remedied in Updates or Upgrades). If the Client is 18 months or more behind in installing Updates or Upgrades, the Supplier may pass on the (demonstrable) additional costs for Maintenance to the Client.

Article 10.17 stipulates that, in principle, the Supplier shall report on compliance with the Service Levels as a matter of course. The Parties may make further arrangements in this regard. Article 10.18 further stipulates that, upon receipt of the report, the Client will assess the extent to which the Supplier complies with the agreements made. Where appropriate, a third party (auditor) may be engaged for this purpose pursuant to Article 27.

Article 10.19 specifies that different provisions apply to the Maintenance of Third-Party Software, provided that these have been notified in good time in advance. In many cases, these different provisions will be determined by the terms and conditions of the holder of the rights to that Third-Party Software. The rationale here is the same as for the entire Third-Party Software regime: because, under the law (Copyright Act)(Auteurswet), the consent of the holder of the rights is

required for any modification to the software (such as in the case of Maintenance), and therefore the Supplier cannot and may not provide any Maintenance whatsoever in the absence of such consent, it is not reasonable to nevertheless include maintenance obligations in the GIBIT.

Article 10.20 forms the final piece of the GIBIT's safety net nature regarding Maintenance. It stipulates that if initially no Maintenance, or only partial Maintenance, was agreed, the Supplier must be willing to perform Maintenance at a later date upon request, or to extend the existing Maintenance Agreement. Naturally, all this is subject to a Fee to be agreed upon. The benefit for the Client lies primarily in the certainty that he can always still proceed to purchase Maintenance.

Article 11. Fees, Invoicing and Payment

Article 11.2 adopts a slightly different approach to that of the ARBIT. Whereas the ARBIT assumes full pre-financing by the Supplier, the GIBIT opts to withhold a portion of the payments until after Acceptance (usually 30%). Arrangements regarding the remaining 70% must be set out in the Agreement.

This is based on the view that it is unreasonable to place the entire financial risk of the project on the Supplier, whilst at the same time ensuring that the Supplier retains sufficient (financial) incentive to ensure the project is implemented correctly. At the same time, it is equally unreasonable for the Client to pay in advance for services that cannot yet be used.

These arrangements result in the following breakdown:

a. 30% of one-off fees is withheld until Acceptance (e.g. 30% of the one-off implementation costs); arrangements are made regarding the remaining 70%;
b. recurring Fees are first payable upon Acceptance of the relevant part of the ICT Deliverable, but are paid in advance from that point onwards (e.g. annual subscription fees);
c. the Fee for Third-Party Software is paid in full upon delivery, provided that the requirements of Article 3.5 have been met.

One-off payments are all payments that are not made on a regular basis. A one-off payment may also be paid in instalments. The Agreement will usually set out in detail how such one-off payments are to be made. For example, the Parties may agree on a payment schedule. However, the GIBIT does not require such details to be specified. Recurring Fees are Fees that become due at regular intervals and with a certain degree of regularity. The Agreement will specify the agreed payment frequency. Examples include monthly, quarterly or annual Fees. In theory, the payment frequency may also be a one-off payment, for example if one final payment is made in the context of extended use (Article 29.11).

The GIBIT stipulates that periodic fees are payable in advance. This is in line with the standard practice of many suppliers (the GIBIT is therefore supplier-friendly in this respect). At the same time, it is also stipulated that the periodic fee is only payable from the date of (partial) acceptance.

The reasoning behind this is simple: it is unreasonable to pay in advance for a deliverable when it is still uncertain whether it meets the agreed requirements (or whether it can be used). Suppliers may perceive this as unfriendly, but that is unjustified. After all, purchasing beforehand and only being paid by one's own customers at a later stage is a standard business risk for a Supplier.

It should be noted that Article 9.4 (concerning the completion of the Acceptance Procedure without delay) applies to both Parties and that commencement of use for operational purposes implies Acceptance (see Article 9.11). Both these nuances can greatly allay any concerns the Supplier may have regarding long-term pre-financing. It is further noted that maintenance fees, which will generally be periodic, are payable only after Acceptance pursuant to Article 10.1, as Maintenance does not start earlier.

Payment is made in advance for the services in the upcoming period (not for the entire contract term). This means that payment must have been made no later than the date specified in the Agreement, or at the latest upon the commencement of that new period. The Supplier cannot

enforce payment at an earlier date (cf. Article 6:39 of the Dutch Civil Code).

GIBIT further acknowledges that, in the case of Third-Party Software, the Supplier is often required to pay directly. This is a procurement relationship in which the Supplier, given the nature of Third-Party Software (which is effectively a monopoly), often has no bargaining power whatsoever (which is different in the case of the procurement of other Products and services). Consequently, in the case of Third-Party Software, there is no withholding of part of the Fee; instead, payment is made after delivery. Incidentally, this applies only to Third-Party Software which has been disclosed to the Client in advance in accordance with Article 3.5. The rationale behind this is to avoid surprises, as Article 3.5 requires transparency in advance.

For the purposes of this Agreement, the time of delivery of Third-Party Software is the time at which the Client is able to exercise actual control over that Third-Party Software (cf. the Dutch Civil Code). Or, more practically speaking: the moment at which the Client is able to use the software. Another moment may, of course, be agreed in the Agreement (such as the moment licences are registered in the Client's name).

The deferred enforceability shall not apply if no Acceptance Procedure is carried out. In conjunction with the rule that use for productive purposes qualifies, in principle, as Acceptance, this provides Suppliers with sufficient assurance in practice that payment will be made on time. If necessary, the Supplier may issue a notice of default to the Client to proceed with the Acceptance Procedure.

Article 11.3 provides an important concession. As described above, the Supplier, as a specialist provider, is expected in principle to be able to meet the requirements set out in relation to Maintenance. However, under certain circumstances, this may prove to be unfair.

The burden of proof in this regard lies with the Supplier. This is a response to questions regarding the costs of processing changes in legislation and regulations, particularly in relation to significant changes to the regulatory framework or (changes announced too late) significant changes to the requirements imposed on ICT Deliverable. It also depends on the extent to which the Supplier, as a party acting with due care and professionalism, could have, or at least ought to have, foreseen the legislative changes. That question cannot be answered in the abstract in these terms and conditions; hence the GIBIT contains only a rule on the allocation of the burden of proof.

Article 11.4 clarifies that the preconditions still apply: any additional work must be reported, the Client must give its approval, and the agreed rates apply.

Article 11.5 provides for the possibility of setting further requirements regarding invoices in the Agreement. Invoices must be issued within three months after the relevant activities have become due and payable. This is to prevent late invoicing, which is in the interests of both Parties. However, the three-month period is not feasible for municipal authorities that are required to close a financial year. It has therefore been stipulated that it is possible to agree that all invoices for work carried out in a given year must be sent to the Client before a specified date in the following year. In the 2023 version, a fixed date of 6 January was specified for this, but this was considered too strict. Consequently, this specific date has been removed. As this date will not be suitable for all Clients, or a strict deadline will not be necessary for all Clients, the inclusion of a fixed end date is merely optional.

Article 11.6 sets the standard payment term at 30 days.

Article 11.7 stipulates that invoices must, as a rule, be issued electronically in accordance with the applicable standard.

Provisions regarding price increases have been introduced in Articles 11.8, 11.9 and 11.10. The main rule is that only the price increase derived from the services price index, group J62 (or at least J6202), may be applied (Article 11.8). Due to the budgetary process of local authorities, it has been stipulated that price indexations must be announced well in advance (one month), including the

specific indexation figure. For this reason, retroactive indexation – for example, because the Supplier has forgotten to send an indexation letter – is not considered appropriate. The index is always compared to the index from 12 months earlier. Consequently, it is also less relevant that the annual index figures may not yet have been published at the time of indexation. Once again, a balance is sought here with regard to Third-Party Software: unforeseeable price increases may be passed on to Clients provided they can be demonstrated. Incidentally, the Parties must bear in mind that price changes may, under certain circumstances, have implications under public procurement law.

In addition, it has happened in practice that Suppliers have increased the price very soon after the contract was signed, on the grounds of indexation. This is considered undesirable, as the Agreement is then concluded on the basis of an unrealistic view of reality. The revised Article 11.9 partially prevents this: in the case of an Agreement concluded at the end of a year, the price cannot be indexed immediately on 1 January. However, this may be deviated from in the higher-level Agreement.

Compared to the 2023 version, the provision regarding the implementation of price reductions has been removed. In practice, it became apparent that this rarely, if ever, actually happened. One of the reasons for this is that the Supplier has little incentive to demand discounts from its supplier if he cannot profit from them anyway. It is also evident that volume discounts based on a certain number of licences are so complicated to implement (after all, Suppliers must calculate which customers are entitled to which portion of the discount) that it is more efficient for Suppliers to dispense with the volume discount. This is understandable, but nevertheless undesirable. The absolute obligation to implement price reductions has thus been removed. This does not mean that Suppliers never have to implement price reductions (this is, of course, never undesirable), but in any case they are not obliged to do so. Suppliers thus benefit from efforts to keep the price of third-party software low, and newly contracted Clients do benefit from the reduced price: after all, the Supplier will quote the reduced price in a new tender. This also provides an additional incentive for Clients to tender carefully and not to allow contracts to run for too long.

Article 11.11 contains a provision regarding unforeseen circumstances that result in a significant increase in costs. The article provides for an obligation to consult and sets out three options in advance: (i) pay the price increase, (ii) limit the ICT Deliverable, or (iii) terminate the Agreement in return for compensation for the costs involved (the latter in view of the reference to Article 24.6). This provision prevents the need to go to court in the event of unforeseen circumstances (cf. Article 6:258 of the Dutch Civil Code).

The bar is set quite high here; we are talking about extreme cases. This article, for example, concerns situations so serious that the continuity of service provision and/or business operations is demonstrably at risk. Whilst allowing a significant price increase is at the discretion of the Client (and not an obligation), in view of the general principles of good governance, a municipal authority can be expected to act reasonably and properly in this regard.

The article also specifies in advance the maximum percentage by which a cost increase is deemed to be at the Supplier's risk (<10%); this provides the Parties with some certainty from the outset. It is, after all, not the intention to regulate matters such as additional indexation in this article. Moreover, the requirements of the Public Procurement Act (Aanbestedingswet) apply in full in this regard, in particular the provision concerning unforeseen costs set out in Article 2.163e of the Public Procurement Act 2012 (Aanbestedingswet 2012). The possibility of a substantial price increase must therefore be applied within the framework provided by the Public Procurement Act.
Article 11.12 stipulates that Fees linked to figures subject to change relating to the Client shall be adjusted only once a year, on 1 January, unless otherwise agreed. The aim is to limit price fluctuations during the term of the Agreement. A different arrangement may, of course, be made in the Agreement.

Finally, Article 11.13 stipulates that the provisions of this article concerning Third-Party Software shall only apply insofar as the Supplier has complied with the provisions of Article 3.5. Article 3.5

stipulates that the Supplier must explicitly specify the relevant Third-Party Software in its quotation. In other words: if the Supplier fails to specify the relevant Third-Party Software, it will not enjoy the benefits of the nuanced payment arrangement as set out in this Article (and therefore, for that Software too, 70% will be paid upon commencement of use and 30% upon full Acceptance).

Article 12. Warranties

The first paragraph of this article sets out various warranties. It is established case law that the Parties' intention regarding warranties is a matter of interpretation. In the case of the GIBIT, the most important intended consequence is set out in Article 12.2, namely that if the Client invokes a warranty, it is then up to the Supplier to demonstrate that such invocation is unjustified. To that extent, the article contains a division of the burden of proof. Furthermore, Article 12.3 specifies exactly what the provision of a warranty entails. This has been done because it is established case law that the meaning of a warranty depends on the parties' intention, whereas that intention will often not be apparent when the Terms and Conditions of Purchase are used in formal procurement processes such as a tender. In the Terms and Conditions of Purchase, these concepts refer solely to the obligation to achieve a result, including the aforementioned allocation of the burden of proof and nothing else.

Most warranties are self-explanatory and primarily ensure that the Supplier guarantees that it will deliver what has been agreed. Compared to version 2023, the warranty that the ICT Deliverable will possess the agreed characteristics and that it will be suitable for the Agreed Use has been removed. This has been removed expressly not because the Supplier is no longer required to comply with this; of course, the ICT Deliverable must comply with the Agreement. However, by formulating this as a warranty, a situation had inadvertently arisen whereby it was up to the Supplier to prove that the ICT Deliverable did not constitute a breach of contract. That is an unreasonable outcome, and was never the intention.

The warranty set out in sub-paragraph (iv) relates to the Client's interest in being able to purchase Maintenance at a later date if necessary. To this end, it is essential that the ICT Deliverable provided continues to be maintained. In this article, the Supplier guarantees that this will remain the case for at least two years following Acceptance.

Article 13. Algorithmic Applications

Municipalities are seeing an increasing use of algorithms, and public concerns about such use are also growing. That is why GIBIT has set out a number of (minimum) requirements for such applications. It is conceivable – and, in certain circumstances, also desirable – that these requirements be further elaborated in the higher-level contract. For the time being, the requirements are limited to the following basic/core requirements.

The first paragraph sets out requirements regarding the algorithmic application (and its quality): lawful data processing, structured and neutral data processing, and accuracy.
The second paragraph includes a restriction on the use of the processed Data: no use for own purposes, unless fully anonymised and non-traceable. If the Data constitutes personal data, the Data Processing Agreement must provide for anonymisation. If the Data are not personal data, then the data must still be non-traceable. This protects commercially confidential and privacy-sensitive information on the one hand, whilst acknowledging on the other that an algorithm requires 'input' for its enrichment.

Given that, in practice, an algorithm is often a 'black box', whilst the municipality, as an actor in a democratic constitutional state, must be able to account for its own actions, paragraph 3 has been amended to stipulate that the Supplier must be able to explain or justify, both in general terms and in specific cases, how the algorithm works or why it has reached a particular decision. This concerns both traceability and explainability. This need not go so far as to require the Supplier to disclose the algorithm (the importance of protecting confidential business information is recognised), but it must go far enough to ensure that, where necessary, the decision can be reviewed in court. After all, the latter is a fundamental principle of a democratic constitutional state. It is therefore important to provide, at the very least, meaningful quantitative and qualitative information. This

means that the model should not merely be explained in technical terms (such as accuracy or error rates), but must (also) be explained in understandable language regarding how the model works and what its limitations are. Ways of complying with this provision could include, for example, the technical possibilities of verifiability, reproducibility and accountability, and the description and minimisation of potential negative consequences. Another option is to shift this obligation from a reactive to a proactive approach, for example in the form of model cards.

In view of the aforementioned principles of the democratic rule of law, paragraph 4 also stipulates that the Client may share information regarding the operation with third parties (such as the court). For the same reason, Article 13.5 also stipulates that the existing right of inspection/audit also applies to the Algorithmic Application (strictly speaking, the provision is almost superfluous, as that right of inspection already applied to the fulfilment of all obligations).

Article 14. AI Systems

New to the Purchasing Conditions is the provision concerning AI systems. It should be noted that this serves as a specification of Article 13: all AI systems are algorithmic applications, but not all algorithmic applications are AI systems. For this reason, a separate article has been created for AI systems.

In drafting this article, the focus was primarily on the AI Act (Regulation (EU) 2024/1689), the EU models for the procurement of AI, and a number of existing procurement terms and conditions in the municipal and healthcare sectors.

The first paragraph sets out requirements regarding the AI system (and its quality): an accurate, robust and secure Product, the operation of which can be verified and the output of which can be understood. This should be interpreted in the same way as the relevant provisions in the AI Act. Principles such as lawfulness, non-bias and transparency are explicitly derived from the AI Act. Should the Supplier be merely the subcontractor and not the provider, the Supplier will have to hold the original provider liable if the latter fails to comply with the AI Act. This does not affect the Supplier's obligation to deliver an ICT Deliverable that meets the specified requirements. The fact that security is included as an explicit requirement for AI systems does not, however, mean that this requirement does not apply to ICT Deliverable that are not AI systems. It is included solely to reflect the text of the AI Act.

The AI Act stipulates that appropriate and targeted risk management measures must be implemented in the AI system. It is conceivable that these may need to be tailored to a specific customer. Paragraph 2 stipulates that the Supplier must be open to this. The exact manner in which this will be implemented will need to be determined through consultation.

Where high-risk AI systems are used, the main obligations rest with the provider. However, pursuant to Article 25 of the AI Act, the deployer may also be regarded as a provider, for example where their name or trademark is affixed to the AI system or where they make a substantial modification to the AI system. It is undesirable to allow municipalities to 'change colour' in this way. For this reason, paragraph 3 stipulates that the Supplier has a duty of care to prevent this 'change in colour', to the extent possible.

Paragraph 4 stipulates that the classification of the AI system (unacceptable risk, high risk, general purpose AI model, etc.) is the responsibility of the Supplier, and that the Supplier must provide evidence or a justification of this upon request. If the classification is 'high', the Supplier warrants that it complies with the requirements set out in the AI Act (paragraph 5). This obligation would have applied even without this provision, but by including it, it becomes a focal point during the contracting process.

The same applies to the logging obligations set out in paragraphs 6 and 7: these obligations arise from the law, but by setting them out in writing, the Parties know exactly where they stand. Furthermore, the Supplier is subject to two obligations to cooperate. Municipalities will have to regularly carry out an assessment of the impact on fundamental rights (FRIA), for which they must

have knowledge of the AI system. The Supplier shall assist in this regard. In addition, it is stipulated that questions regarding the operation of the AI system and the interpretation of output fall within the remit of User Support (helpdesk).

Finally, the Client is also expected to assist the Supplier. The AI Act sometimes requires users to be informed about the AI system, so the Client will also need to do this at the Supplier's request. Furthermore, the Client can assist the Supplier by providing feedback on the functioning of the AI system.

Naturally, the provision of an AI system cannot be viewed separately from its use. The Supplier cannot be held liable for any (incorrect) applications that the Client assigns to the AI system itself. Article 36 provides a basis for this.

Article 15. Documentation and Information

The first paragraph of this article stipulates that the Supplier must provide Documentation. The article also sets out a number of requirements regarding the Documentation, in paragraphs 1, 2 and 3.

Documentation is used here in a broad sense: the article relates to the use of the ICT Deliverable provided (sub-paragraphs i and iii), the documentation of the settings made by the Supplier (sub-paragraph ii), the ability to carry out acceptance tests (sub-paragraph iv) and the management of the ICT Deliverable (sub-paragraph v). In this regard, the GEMMA Software Catalogue (www.softwarecatalogus.nl) may be used in part to comply with sub-paragraph (v).

To allow Suppliers sufficient flexibility, it has been stipulated that only Documentation intended for end users must be in Dutch. Other Documentation may also be drafted in English.

Article 15.4 concerns the timely provision of the Documentation. The article stipulates, in general terms, that the Supplier must update the Documentation as soon as it becomes apparent that it is no longer accurate. The initiative for an Update may come either from the Supplier himself or from the Client.

Article 16. Product Management

It is important for Clients to be kept informed in a timely manner about developments relating to the ICT Deliverable. That is why this article specifies that the Client must be informed of the roadmap in a timely manner (Article 16.1) and be granted access to forums/platforms where experiences with and information about the ICT Deliverable are exchanged (Article 16.2). Both aspects are separate from any agreed Maintenance.

Article 17. Liability

The issue of liability often leads to heated discussions between Clients and Suppliers. However, experience also shows that these discussions are not always justified:

a. On the one hand, Clients must realise that it is their responsibility, as bodies governed by public law, to apply a proportionally appropriate contractual framework. The GIBIT has sought to provide a starting point for this by applying a liability cap that is proportional to the contract value (as in ARBIT). This does not preclude the possibility that, where appropriate, it may be necessary to deviate from this framework.
b. On the other hand, Suppliers must realise that any failure on their part may result in significant losses for Clients and that it is therefore not unreasonable for Clients to require Suppliers to compensate them for any losses caused by the Suppliers and for Suppliers to hold appropriate insurance cover for this purpose. Suppliers may also be expected to have organised their business operations in such a way that an incident does not immediately lead to disproportionately large losses or losses affecting a large proportion or all of the customers of those Suppliers.
c. Both Parties must also be aware that, in addition to the provisions of the GIBIT, the Dutch Civil Code (and other legislation) applies in full, unless the GIBIT expressly provides otherwise. This means, amongst other things, that the rules set out in Book 6, Title 1, Section 10 (on compensation) apply, including the rules contained therein regarding the assessment of

damages, causality, contributory negligence, etc. Thus, the Client may only claim damages if there has been a breach or wrongful act on the part of the Supplier and may not claim damages to the extent that the Client is himself at fault or to the extent that the damage lacks a sufficient causal link to the Supplier's breach. Contrary to what is sometimes claimed in negotiations, there is certainly no question of unlimited liability (but rather liability limited by the framework of the Dutch Civil Code.

The liability article distinguishes between personal injury and property damage on the one hand, and other damage on the other. This distinction between these two types of damage is in line with insurance policies available on the market. As such, no distinction is explicitly made between direct and indirect damage. This distinction does not exist in Dutch law and it is (therefore) often unclear exactly what is meant by the distinction. Uncertainty is not in the interests of either Party. Sometimes, indirect damage refers to damage that lacks a sufficient causal link to the breach; however, the requirement of a causal link is an established rule of Dutch tort law (see above).

The remaining damages are calculated in relation to the amount of the Annual Fee. The term 'Annual Fee' is defined in Article 1. Essentially, it refers to the annual average of the (originally envisaged) total fee, calculated over the (originally intended) duration of the project. In practice, that total price will often be based in part on one-off fees, periodic fees or fees calculated on a subsequent calculation basis. To provide clarity for both Parties, it has been stipulated that the amount of these fees must be calculated on the basis of the initially intended duration and the initial budgets. In this way, Parties will know – prior to concluding the contract – what the extent of the maximum liability will be in any given case. A more dynamic definition has deliberately not been chosen, as this would only lead to uncertainty in practice. The Parties should therefore be aware that, in the event of major changes to an existing Agreement (to the extent permitted under public procurement law), it is likely to be appropriate to adjust the liability regime.

The maximum liability is twice the Annual Fee per incident, and the maximum total liability per year is four times the Annual Fee. Regardless of this 'safety net', the Parties will, of course, always be required to reach proportional agreements. Other arrangements are therefore also conceivable.

Often, the discussion begins with a view to including not only a limit on liability per incident but also an overall limit on liability. The working group is critical of these requests. Such agreements could, in fact, result in there being little incentive for the Supplier to fulfil its obligations in certain situations (after all, with an absolute maximum, the Supplier is no longer liable once that maximum has already been 'reached' due to previous claims). That is why it has been decided to limit the maximum liability to a period of one year at a time. In the following year, the proverbial counter will be reset to zero (a clean slate). This is also consistent with the system used by insurers. Furthermore, the interests of Suppliers are served by the provision that related events are treated as a single event. The working group believes that this represents a balanced approach that serves both interests: on the one hand, a realistic and sufficiently high maximum for Clients that provides sufficient incentive for compliance; and on the other hand, an absolute annual maximum for Suppliers, which is therefore also more predictable and insurable.

Paragraph 5 sets out a nuanced provision regarding exceptions to the liability regime, taking into account the Proportionality Guide. Essentially, this brings together all the usual exceptions to the limitation of liability. Limiting liability in the event of death or personal injury (sub-paragraph i) and in cases of wilful misconduct or gross negligence (sub-paragraph ii), is generally considered unacceptable. Infringement of IP rights (sub-paragraph iii) falls entirely within the Supplier's sphere of risk by its very nature, as the Client (who receives only object code) is not in a position to verify whether the Supplier is infringing any rights. Furthermore, the Supplier is already entitled to intervene himself to limit such damage (see Article 21). The exception to the limitation for the processing of personal data in sub-paragraph (iv) is nuanced. The ARBIT opts for unlimited liability in the event of shortcomings relating to the processing of personal data. However, this does not seem to be proportionate in many cases. For this reason, sub-paragraph (iv) of the GIBIT stipulates that no limitation applies only to fines that could also have been imposed on the processor (thereby emphasising that the fine must relate to actions falling within the Supplier's sphere of risk) and on

condition that the Supplier shall be informed in good time of any investigation by the supervisory authority and shall be involved in mounting a defence against the fine. One example of this is a situation where the Supplier has inadequate security measures and the Client consequently suffers a data breach: the Client may be fined for the data breach, but this is beyond his control. In such a case, it would be unfair if the Supplier could then invoke the liability cap.

It is, incidentally, explicitly stated that the Supplier 'shall be involved in' mounting a defence against the fine, and not something like 'coordinating'. After all, it is ultimately up to the Client himself to determine whether, and if so to what extent, a defence is to be mounted against a fine imposed on the Client. However, set against that party autonomy is the fact that, according to standards of reasonableness and fairness, it would be unacceptable to, on the one hand, seek to recover the fine from the Supplier whilst, on the other hand, not allowing that same Supplier to mount a defence against (the part of the fine attributable to the Supplier). That would amount to a kind of 'blank cheque' situation, which is not the intention. This nuanced set of preconditions must therefore be viewed in that light.

It should be noted that a decision has been taken to keep the number of exceptions to the liability provisions to a minimum. Other terms and conditions of purchase, for example, stipulate that the limitation of liability is waived in the event of data breaches. In the GIBIT, it has been decided not to make this a (generic) exception. This does not mean that the working group is of the opinion that not excluding data breaches is always the appropriate course of action. It is advisable to assess on a case-by-case basis whether an exception for data breaches is proportionate.

Article 18. Insurance

Article 18 specifies that the Supplier must provide adequate security for recourse, either through insurance or by other means. A conscious decision has been made not to make insurance mandatory. After all, there are countless ways in which the risk to Clients that the Supplier may not provide recourse in the event of a claim can be covered (parent company guarantee, bank guarantee, escrow account, etc.). Sometimes this means that the Supplier must be insured for professional and business liability, but in certain cases it may also be appropriate and customary for the Supplier to have cyber insurance.

The second paragraph sets out a minimum level of cover, both in terms of the amounts to be paid out and the number of events per year. This cover corresponds to the maximum liability as set out in the previous article.

Article 19. Confidentiality

Article 19 sets out a mutual obligation of confidentiality. The first paragraph stipulates that both Parties shall keep confidential all information of which they are (or ought to be) aware of the confidential nature, with an exception for subcontractors, shareholders, auditors, professional advisers, and the like. The Parties are also released from the confidentiality obligation to the extent that this is necessary on the basis of a statutory requirement, an investigation by a supervisory authority, or legal proceedings.

The second paragraph sets out the minimum confidentiality period. Where necessary, this period may be extended, depending on the nature of the data. In any event, the period specified in the Data Processing Agreement shall apply to personal data.
The third paragraph stipulates that both Parties shall also impose confidentiality on any Staff and auxiliary personnel engaged by them.

To ensure transparency within the public sector, the fourth paragraph has been amended to state that the content of Agreements may be shared within municipalities, between municipalities and with relevant partners. In this way, the GIBIT is more in line with, for example, legislation on open government.

Article 19.5 stipulates that confidential data must be returned upon request. This obligation, like the other obligations set out in this article, is separate from the obligations incumbent upon the

Supplier under the Data Processing Agreement. Furthermore, the Supplier cannot, of course, be expected to delete data if doing so would violate the law, such as statutory retention periods.

Finally, paragraph 6 imposes a penalty on all Parties for breaching the duty of confidentiality. A penalty has been included because, in practice, it is often difficult to quantify the damage caused by a breach of confidentiality. Consequently, without a penalty article, there might be no incentive to keep confidential information secret (after all, if the damage cannot be quantified, no claim for damages can be made).

Article 20. Force Majeure

The first paragraph of this article essentially reiterates the provisions of the law regarding force majeure.
The second paragraph specifies that certain circumstances shall in any event not be classified as force majeure. The circumstances mentioned in this paragraph are therefore at the Supplier's risk. This is, of course, subject to reasonableness and fairness: although illness is not force majeure, this does not mean that the Client may seek to create a dispute with the Supplier if a member of staff occasionally has the flu.

A nuanced approach has been adopted with regard to the failure of utility and telecoms services. In principle, the failure of such services constitutes force majeure. The GIBIT thereby acknowledges that Suppliers themselves also procure such services and are often not in a position to enforce a certain level of service provision. However, force majeure does not apply if the disruption was caused by the Supplier himself or if it has been agreed that the Supplier was required to keep the utility or telecoms services available. To illustrate the latter: for a cloud/ASP service, this usually means that the Supplier may be held liable if his own connection to the public internet fails (this is then not force majeure), but not if there are disruptions on the public internet or at the Client's provider that prevent the cloud/ASP service from being used.

Article 20.3 stipulates that the Supplier must compensate the Client for any benefit gained as a result of force majeure, subject to the limitation of liability. The rationale is simple: the Supplier should not benefit financially from a situation of force majeure. This provision has been taken from the ARBIT.

Article 21. Intellectual Property

The GIBIT aligns with the distinction commonly made in the market between standard and customised work: in principle, the rights to standard services rest with the Supplier, and the rights to Customised Software with the Client. This also applies to the rights to Data. This is laid down in Article 21.2, to ensure that copyright and database rights vest in the Client. Incidentally, Article 13.2 subsequently grants the Supplier the right to use that Data, notwithstanding those IP rights (provided it has been anonymised).

In the case of Customised Software, the software is developed specifically for the Client. It therefore stands to reason that the Client should also be granted the rights to and access to the source code of that work. This is stipulated in Article 21.4.

A Licence is granted in respect of the other ICT Deliverable. This is set out in Article 21.3. The term of the Licences varies depending on the nature of the Fee: in the case of periodic Fees, the term of the Licence is equal to the term of the Agreement; in the case of other Fees, the Licence is perpetual. The link to the duration of the Agreement (and not to the payment frequency) in the case of periodic Fees is deliberate; the aim is to prevent late payment from automatically leading to the expiry of the Licence. This abstract description is also in line with a multitude of licensing models that exist in practice. The (higher-level) Agreement concluded between the Parties will determine which licence model will be applied in specific cases. However, it is established in advance – partly at the request of Suppliers – that a licence does not, in principle, include the right to carry out acts of exploitation oneself. The term 'acts of exploitation' is very broad and is also commonly used in IP literature.

Paragraph 4 sets out the delivery and transfer of ownership for Customised Software. Compared with the 2023 version, a new principle applies here: 'open source, unless' (paragraph 5). This is elaborated on in Chapter IV.

It is also conceivable that several municipalities could jointly ask the Supplier to develop Customised Software. The law stipulates that this would result in shared intellectual property rights. It is conceivable that this might not be desirable at all, as it would be more practical to assign these rights to a single municipality (the driving force), for example. This is explicitly set out in paragraph 6.

Paragraph 7 provides that the Supplier shall indemnify the Client against claims arising from infringements of intellectual property rights and related rights (such as moral rights and rights of publicity).

Paragraphs 8 and 9 ensure that the Client may continue to use the relevant functionality in the event of claims by third parties that the ICT Deliverable in use infringes their rights. In the event of an infringement, the Supplier must provide a solution as soon as possible, choosing from at least one of the options set out in paragraph 8.

Paragraph 10 stipulates that, in the event of a claim for liability by the third party concerned, the Client must also be able to terminate the Agreement. This provision is intended, in particular, to limit the damage suffered by the Client. The Client must, after all, record a claim for liability in its records and thus has an (accounting) incentive to cease the (alleged) infringement as quickly as possible. In practice, recourse to paragraph 10 is unlikely to be frequent, and the (more practically oriented) approach of paragraphs 8 and 9 will be particularly relevant.

The provision in paragraph 10 allowing for the termination of the Agreement following an alleged infringement of intellectual property rights by third parties (see also 17.5), has been included due to the potentially significant consequences of such a claim. As a result, the Client may face, amongst other things, the seizure of all infringing items, including computers on which infringing software is installed. Furthermore, the (alleged) rights holder may claim damages for lost licence fees. The fact that an allegation is sufficient for termination, and that no judicially ascertained infringement of intellectual property (IP) rights is required, is due to the fact that the costs (see above) can rise very quickly in the event of a continuing infringement of IP rights, whilst legal proceedings to definitively establish the infringement can take a very long time.

Finally, Article 21.11 stipulates that the warranties and indemnities relating to IP infringements shall not apply if they relate to works made available by the Client to the Supplier or to modifications to the Supplier's Software made by the Client himself

Article 22. Access to Data and Authorisations

Compared to the 2023 version, the article on Data has undergone significant changes. In light of new and renewed attention to the role that data plays within the public sector, the Terms and Conditions of Procurement respond to developments in the market. The aim is for the provisions regarding Data to comply with the Open Government Act (Wet open overheid), the Reuse of Government Information Act (Wet hergebruik overheidsinformatie), de Data Act (2023/2854), de Data Governance Act (2022/868) and other new developments. It is, after all, of great importance to Clients that they retain access to the Data (their own Data) processed as part of the ICT Deliverable. Clients also wish to be able to use the relevant data outside the scope of the deliverable provided by the Supplier and/or for other purposes and in other processes and systems, such as business intelligence applications or big data analyses for management information and/or in business systems that form part of the process and information chain. They must also comply with statutory (transparency) obligations.

This article applies not only to personal data, but also to non-personal data. Furthermore, this article applies not only to 'traditional' data processing (SaaS services), but to all physical and digital products and services through which data is generated and processed. This includes, for example, not only smart cameras and civil affairs applications, but also traffic lights that count the number of

cars passing by, and playground equipment that tracks usage.

In this context, paragraph 1 of Article 22 stipulates that the Supplier must inform the Client that Data is being processed. It should not be the intention that Suppliers generate Data (and use or sell it themselves) without the Client being aware of this.

Paragraph 2 stipulates that, in principle, this Data must also be shared with the Client. It is up to the Parties themselves to reach agreements on this. Access to a portal is one option, but it is also possible for the Supplier to periodically retrieve a Product and transfer the Data to the Client. In the case of Data of a dynamic nature (such as sensor data), for example, it makes sense to make the Data accessible via an API. When determining the method of provision, the parties may also consider agreeing on a licensing model for the Data. CC BY or CC0 are among the options available for this.

This data provision must then be carried out in a standardised and clearly explained manner (22.3). It is the Supplier's responsibility to use robust data structures that enable the Client to meet its legal obligations. This does not, of course, preclude the Client from assisting in this regard, for example by explaining which data structures work best for him. It may be the case that Data cannot be interpreted without access to the underlying model or metadata model.
However, if this model is disclosed, trade secrets may be revealed. It is explicitly not the aim of the GIBIT to compel Suppliers to disclose their trade secrets. Therefore, the Supplier may require that an NDA be signed by anyone who is granted access to the description of the data model. This must, however, have been communicated in advance; it cannot be the case that the Client discovers this, for example, in the middle of a Woo process.

The Client is, subsequently, free to use the Data at its own discretion, unless the Supplier holds intellectual property rights over it (22.5). Furthermore, incorrect Data must be corrected (22.6) and the Supplier shall assist with the interpretation of the Data (22.7). The right to correction is intended for situations where the Data are technically incomplete or incorrect, for example because they have been incorrectly converted. It is not intended that the Supplier should be expected to supplement the Data himself free of charge or to correct errors made by the Client.

Paragraph 8 stipulates that the Data, in the same way as applies to personal data under the GDPR, is processed on behalf of the Client. Consequently, the Supplier shall use the Data solely for the performance of the Agreement, shall not delete the Data without being instructed to do so, and shall delete the Data as soon as instructed to do so. Upon termination of the Agreement, the Parties shall consult on the consequences of such termination for the processing of the Data. It should be noted that this paragraph, like all other provisions in the Terms and Conditions of Purchase, may be deviated from. This means that the Parties may, for example, agree that the Supplier may use the Data (other than personal data) for its own purposes, or that the Data will be automatically deleted or overwritten.

Paragraph 9 stipulates that the foregoing does not apply in four cases. Firstly, this does not apply if compliance with the obligation is technically impossible, for example because the Data is stored with a third party and the Supplier does not have access to it either. This must, however, be impossible at all times; the mere fact that the Supplier deletes the Data, for example, does not affect the application of Article 22. Secondly, the Data are not required to be shared or removed in breach of the law. Thirdly, the Supplier need not disclose its trade secrets. It is, however, up to the Supplier to prove that this is the case. Finally, the Supplier need not do anything with the Data if the Client has indicated that it does not need to receive the Data.

The final paragraphs stipulate that the Client uses the Data at its own expense and risk. However, the Supplier must warn the Client if granting access results in certain security measures being circumvented (paragraph 10). This enables the Client to make an informed decision regarding the use of the Data.

Article 23. Third-Party Software

The GIBIT contains a separate provision regarding third-party software. This term is defined in Article 1. It refers to software from external suppliers who are not affiliated with the Supplier and over the development of which the Supplier has no influence. Examples include software from parties such as Microsoft, Oracle, Adobe, Google, IBM, HP, SAP, etc. Incidentally, certain open-source software may also fall under this definition.

The provision in Article 23 has been included in recognition of the fact that Suppliers generally have no influence over the quality or functionality of this Third-Party Software, nor over the terms and conditions under which it is placed on the market. This is linked to the legal provisions on copyright, from which it follows (in essence) that it is exclusively for the rights holder to determine whether, and if so under what conditions, software is placed on the market and under what conditions this software may subsequently be used.

For the same reason, no provision has been expressly included regarding 'third-party equipment' or similar items. This is because the legal regime governing physical goods (such as hardware) differs from that governing software. The basic principle in the sale of movable property is, after all, that the purchaser is free to use and resell those goods, whereas, from a legal perspective, that freedom does not exist with regard to software. A seller of defective goods will normally also be able to take legal action against the underlying supplier (have a right of recourse against their supplier).

Although experience shows that much third-party software is also available from other suppliers, or may already have been purchased by the Client, the working group does not consider it part of the Supplier's duty of care to actively inform the Client of the possibility of obtaining third-party software elsewhere.

The first paragraph stipulates that the Supplier must release Updates and Upgrades in a timely manner in order to continue to ensure compatibility with Third-Party Software. This could, for example, refer to a situation where the IT Deliverable ceases to function following an Update to the Third-Party Software, or a situation where the Third-Party Software itself (for whatever reason) ceases to function.

The provisions of paragraphs 2 and 3 constitute the final clause regarding the dependency on third-party software. In essence, those paragraphs state that a Supplier is not liable if a Defect in the deliverable he has provided (usually software) is caused by an error in the third-party software, unless the Supplier ought to have been aware of that error and could have worked around it. Any agreed Service Levels and the like therefore do not apply in that case either. However, the Supplier must still do everything in its power to resolve the problem as quickly as possible (paragraph 3).

The Supplier cannot benefit from this (generous) exception to the maintenance obligations if it has not provided the information specified above. In such a case, the Supplier is, in principle, also in breach of the relevant obligations. This could, in principle, justify the termination or possible annulment (on the grounds of error) of the Agreement. However, it must always be assessed on a case-by-case basis to what extent the Supplier's withholding of the relevant information has been a determining factor to the situation in question.

Paragraph 4 provides for an exception to this regime for Remote Services. In an on-premise situation, the software is installed on local equipment and the running of the program constitutes in itself an act subject to copyright for which a licence is required (cf. Section 45i of the Copyright Act) (Auteurswet). In that situation, therefore, both the Supplier's software and the third-party software (e.g. an SQL server) are installed, and the Client requires a licence for both packages. Since that licence is in practice non-negotiable (neither for the Supplier nor for the Client), the Terms and Conditions of Purchase recognise that those licence terms and conditions shall prevail. The Supplier may then pass these on directly to the Client. Furthermore, Article 23 acknowledges that Defects caused by bugs in that Third-Party Software are not (attributable) Defects, but that the Supplier must nevertheless devise a solution as soon as possible.

The situation is quite different in the case of Remote Services (cloud, SaaS). In this case, the software is installed on the Supplier's server. It is the Supplier who carries out acts of reproduction (by running the software) and who (therefore) requires a licence. Whereas in the on-premise situation it is the Client himself that requires a licence for that third-party software (such as an SQL server), in the case of Remote Services it has become an internal matter for the Supplier to ensure it holds the correct licences. The Client simply purchases a complete package as a service. The Client does not see which third-party software is being used, nor does it use this software itself. It only uses the Supplier's package.

Paragraphs 5 and 6 address situations where the use of the Third-Party Software changes, for example where the licence terms and conditions change (paragraph 5) or where additional Third-Party Software is taken into use (paragraph 6). It is possible, after all, that a Supplier may offer additional Products during the term of the Agreement, for example in the case of purchase on demand or when offering an additional module.

In both situations, it is up to the Supplier to be transparent and to provide and explain the (new version of) the licence terms and conditions. The Client's administration must, after all, remain complete, meaning that if third-party terms and conditions change, the Client must also have access to them.

Paragraph 7 deals with the role of the broker as municipalities are increasingly making use of brokers. Whilst this is efficient, it raises complex issues under public procurement law. Furthermore, in this triangular relationship, there is a risk that whilst the Terms and Conditions of Purchase apply between the Client and the broker, they do not apply to the ultimate supplier. This is problematic, as the actual risks will mainly arise within the sphere of risk of the ultimate supplier (data breaches, liability, breach of contract, etc.). This paragraph clearly states that the broker must ensure that the GIBIT apply between the Client and the supplier. If this is not possible or not appropriate, the broker must first consult with the Client. The Client may then also give permission to deviate from certain provisions at all times (e.g. to always accept a lower level of liability) or to declare the GIBIT not applicable to certain suppliers or certain ICT Deliverables, but this must first be discussed and recorded in writing.

Article 24. Replacement of Personnel

The article on the replacement of personnel has been taken from the ARBIT, except for the prohibition on replacing personnel without permission, which has not been included. The provisions are procedural in nature and are largely self-explanatory.

Article 25. Software Bill of Materials

A new feature of the Terms and Conditions of Purchase is the Software Bill of Materials (SBOM). Requirements regarding cybersecurity and the supply chain are becoming increasingly stringent, for example under the Cyber Resilience Act (Regulation (EU) 2024/2847). The Supplier is therefore required to be transparent about its supply chain and dependencies. This is achieved in the form of a Software Bill of Materials. This article aligns as closely as possible with the guidelines of the NCSC. The Supplier is required to be transparent about the use and origin of third-party software, the supply chain and the recipients of the Data. The working group recognises that the SBOM is not necessary in every situation. As with all other provisions in the Terms and Conditions of Purchase, it is possible to deviate from this provision in the Agreement or to declare it inapplicable. It is the Client's responsibility to apply the SBOM obligation in a proportionate manner. If something is not part of an essential chain, the SBOM obligation will not always be obvious. For example, it is obvious to require a comprehensive SBOM for critical infrastructure (such as civil affairs applications and financial software packages), applications that remain in use for a long time, ICT Deliverables with many integrations and interfaces, and systems with high compliance requirements. A comprehensive SBOM is less obvious in the case of, for example, small ICT deliverables (such as a plug-in), non-critical services (such as a translation tool) and publicly available open-source software.

In 2025, the SBOM is a relatively new concept, meaning that there are not yet numerous market standards in place. One of the market standards that does exist is ISO/IEC Standard 5230:2020. To avoid creating unnecessary compliance obligations, it has been specified that compliance with this standard is sufficient (paragraph 2). The Supplier may therefore choose to provide an SBOM as referred to in paragraph 1, or to be certified under the ISO/IEC standard and provide evidence of this. As this standard allows for self-certification, this is a relatively accessible way to develop a uniform SBOM. Furthermore, the purpose of the SBOM is to enable the Client to identify where dependencies, licensing issues, bottlenecks and other risks lie. It is, therefore, not acceptable to leave fields from the standard blank.

The purpose of the SBOM is to stimulate cybersecurity. If sharing part of the SBOM were to create a risk to cybersecurity, this objective would be undermined. This is thus not the intention, as stipulated in paragraph 3. Providing a complete SBOM may indirectly reveal the applied architectural and supplier choices (such as strategic dependencies) and components or versions which, although not publicly vulnerable, may be susceptible to misuse or reverse engineering. A Supplier is not obliged to share this, unless it is necessary in the wake of an incident (for example, to take effective measures against (further) damage). It should be noted, however, that this will almost never be the case: research shows that SBOMs do not pose a security risk in practice. This is all the more true because the SBOM is strictly confidential (paragraph 4).

Finally, the role of the IBD as a CSIRT is specified in paragraph 5. It is conceivable that, in future, communication regarding cybersecurity will (to a much greater extent) be channelled through the IBD. This is beneficial for both parties: municipalities can draw on the expertise of a highly specialised organisation, and suppliers will only need to liaise with a single party regarding cybersecurity, rather than with all their customers.

Article 26. Company Takeover

There is often some unease in the market when the Supplier's company is taken over. There is often little cause for concern, but there is a great deal of uncertainty regarding the consequences of such a takeover. This article has been included to alleviate this concern. It does not introduce any new requirements (compliance with the law and with the contract is always required), but provides guidance for discussions regarding the takeover of a company.

Article 27. Suspension, Termination and Dissolution

The GIBIT sets out a number of additional provisions to the legal provisions governing suspension, termination and dissolution. The other legal provisions therefore remain in force.

These are three legally distinct remedies/situations, which essentially boil down to the following:

- suspension = pausing. The Agreement remains in force, but one of the Parties pauses its own work in response to the conduct of the other Party. The most common situation is one in which one Party first fails to fulfil its obligations, in response to which the other Party pauses its related obligations (cf. Article 6:262 of the Dutch Civil Code). An example of this is pausing work in response to a failure to make timely payment.

- termination = cancellation. The Agreement is terminated and the Parties part ways, without any claims for damages. This is only possible at the end of the term. Early termination will result in liability for damages. In the case of long-term relationships or a high degree of dependency, it is conceivable that an extended notice period may need to be observed.

- dissolution = reversal + compensation. The Agreement comes to an end and the effects of the Agreement are reversed as much as possible. In practical terms, this means that the goods supplied are returned and the money is refunded. Where return is impossible, the value of the deliverable to the recipient is assessed. That value may range from the fees paid down to 0. In the event of termination, the loss suffered as a result of the breach and the termination may be recovered from the other party. Termination is only possible if the other party fails to fulfil an obligation or if another ground for termination arises. Termination may also be partial.

These additions have been included for the benefit of the Client. For example, the Supplier's right to invoke suspension has been restricted (Article 27.1). This is because the Client is often heavily dependent on the Supplier, whereas the legal system allows the Supplier to invoke suspension with relative ease. In the event of a potential invocation of suspension, the Supplier must give prior warning of the consequences thereof. This constitutes a further elaboration of the (already applicable) duty of care and, moreover, is simply a matter of common decency.

Article 27.2 stipulates that fixed-term contracts may not, in principle, be terminated before their expiry, and that contracts of indefinite duration may, in principle, always be terminated subject to the notice periods specified. This provision is linked to the provisions of Article 7:408 of the Dutch Civil Code.

Article 27.3 stipulates that, despite their interdependence, related Agreements may be terminated selectively at the end of their current term. An example of this would be terminating the maintenance agreement whilst the agreement for Remote Services continues. The provision may, incidentally, also be interpreted as allowing for selective renewal. The article is primarily intended to remove any doubt as to whether, by virtue of their interdependence, the Agreements must necessarily be renewed or terminated simultaneously. The article expressly does not concern early termination.

Articles 27.4 and 27.5 stipulate that the Client must be able to terminate the Agreement(s) in the event of a merger, outsourcing or a mandatory switch to national facilities. The rationale behind all these provisions is that, without such authority, the Client would not be able to terminate existing Agreements where necessary and would therefore have to continue paying for services that are no longer of any value to him. Article 27.6 stipulates that the Supplier is entitled – in short – to charge the Client for the loss thereby incurred. When calculating such damages, account must be taken of the Supplier's potential re-utilisation of production resources. This is to prevent the Supplier from receiving compensation from the Client for this production resource whilst simultaneously generating a profit from it again (with another customer).

Articles 27.9–27.13 set out the various grounds for termination in detail. In addition to the statutory grounds for termination, the usual grounds (such as the Supplier's bankruptcy) have also been included here. Provision is also made for termination in the event of an Agreement being annulled under the Public Procurement Act and in the event of a prolonged force majeure. Provision is also made for the situation where there is a desire to terminate the Agreement if its continuation would be contrary to fundamental rights and the rule of law. This is in line with the Digital Fundamental Rights Agenda (Agenda Digitale Grondrechten) and the principles of CSR. To prevent arbitrariness and legal uncertainty regarding the latter ground for termination, the burden of proof that continuing the Agreement would be unacceptable lies with the Client. This ground for termination is intended only for the most extreme cases.

These are all situations in which the Client cannot reasonably be expected to continue the Agreement. Naturally, when invoking any of these grounds for termination, it is for the Client to prove that these grounds actually exist. Furthermore, Clients who wrongfully invoke termination are liable to the Supplier. There is therefore certainly no question of the 'easy escape' as feared by some Suppliers.

In all cases, the statutory principle that, in principle, services rendered are to be reversed (including the repayment of Fees paid) has not been departed from in relation to termination. This is because that same Act also establishes the principle that, to the extent that the services rendered have been of value, the Fee remains payable to the extent of that value. The law is therefore already (very) nuanced. For example, in the event of termination due to the Supplier's bankruptcy, it would certainly not be obvious that past Fees should also be refunded, since these were, after all, in return for services that will have been of value.

Furthermore, there has been no deviation from the basic legal principle that termination is not possible in the event of creditor's default on the part of the Client.

Article 28. Right of Inspection and Cooperation with Audits at the Client's Premises

This article relates to two different (and unrelated) types of inspections/audits: on the one hand, the Client's inspection of the Supplier (paragraphs 1–5) and, on the other hand, the Supplier's cooperation with audits carried out at the Client's premises (paragraph 6).

The Client is entitled to have an independent (non-competing) third party verify whether the Supplier is fulfilling the agreed obligations (paragraph 1). The accuracy of the invoices may also be examined (paragraph 1).

In the interests of reasonableness, it has been added that the inspection must relate to compliance with essential obligations. For the same reason, it has also been added that an inspection is only justified if there is reasonable doubt as to the Supplier's compliance, or if there is another legitimate interest on the part of the Client. The reason for an inspection must also be disclosed. This enables the Supplier to provide information and thereby potentially remove the reason for the inspection. Paragraph 2 also stipulates that the generic TPM must first be requested before an inspection may take place. Finally, the inspection must take place within a reasonable period of time and the auditor is bound by confidentiality.

The Supplier must cooperate with the inspection to the extent that can reasonably be expected (paragraph 3). The costs of the inspection shall be borne by the Client, unless the expert identifies relevant breaches on the part of the Supplier (paragraph 4). This last provision means that a Client will be cautious and prudent regarding the number of inspections to be carried out.

The role of the IBD as a CSIRT is also mentioned in this article, specifically in paragraph 7. It is conceivable that, in future, communication regarding cybersecurity will (to a much greater extent) be channelled through the IBD. The monitoring of this can also be centralised. This is beneficial for both parties: local authorities can draw on the expertise of a highly specialised organisation, and suppliers need only undergo a single inspection, rather than one by each of their clients. In the case of an inspection by the IBD, it is not mandatory to first establish reasonable doubt, as this inspection is, by its very nature, less incident-focused.

The Client may also be subject to audits. In that context, it may be relevant to be able to provide further information regarding the ICT deliverables used. In most cases, the Client will be able to provide that information without the Supplier's cooperation. However, there may be circumstances in which the Supplier's cooperation is necessary. For such circumstances, paragraph 8 stipulates that the Supplier shall cooperate fully with any such audit.

Article 29. Exit plan, Transition, Limited Continuation, Transfer and Extended Use

Article 29 forms the final part of the GIBIT's 'life cycle' approach. This article describes various situations in which the Client no longer uses the ICT Deliverable and what needs to be done (in preparation for this) to ensure a smooth transition.

Article 29.1 stipulates that, at the request of either Party, the Parties shall draw up an Exit Plan, and that an existing plan may be required to be updated. In principle, this takes place once a year, but the Parties may deviate from this. An up-to-date plan is, after all, in the interests of both Parties. Incidentally, this is not intended to encourage the Supplier to convene an unnecessary number of meetings regarding the Exit Plan as a means of generating revenue. As a general rule, it may be assumed that the Client will reimburse the Supplier for hours worked if the Client convenes the meeting, but the Supplier will offer the meeting free of charge if the Supplier is the one convening it.
This article relates solely to the drafting of the plan as such. The plan may set out in more detail one or more of the options described in the following paragraphs. It is clear that the provisions of the Terms and Conditions of Purchase are intended as a safety net; ideally, the Parties should draw up a more specific plan.

The first option described in this context is that of the transition to a similar ICT Deliverables (Articles 29.5–29.7). This scenario concerns the switch to a different system, or the transfer of the

management of the existing system to another party. The Supplier is obliged to cooperate with this. The aim is to prevent a vendor lock-in situation. An exit can be complex under certain circumstances. It is therefore advisable to evaluate/test the exit in advance. This is to prevent unforeseen circumstances from suddenly arising when the time actually comes. The Supplier may charge fees for the evaluation.

The second option described is the acquisition of new licences for limited use (Articles 29.8–29.9). The idea is that the existing (broad) licences are no longer necessary, but that the Client can, by means of more restricted versions of (new) software or restricted licences for the existing software (e.g. view-only rights, no use of the software), at least still secure a basis for accessing certain Data. It is also stated here that it must in any event be possible to comply with the duty to keep records; here too, a proportionate approach must be taken in every instance. If, for example, the Client requires the Supplier to continue offering limited access throughout the full seven (7) -year tax retention period, the Client may in certain cases be expected to be willing to consider alternative methods of providing access to the records.

The third option available involves transferring the ICT Deliverable to a joint arrangement or other public entity (Article 29.10). This article applies in addition to the provisions of Article 27.4. The latter article provides grounds for terminating the Agreement, whilst Article 29.10 provides grounds for transferring the Agreement. This means that the Exit Plan set out in Article 29.1 applies to these activities. What this means for the prices of the ICT Deliverable will, as with all matters relating to prices, depend on what the Parties have agreed in the Agreement and/or the Price List. If a fixed fee has been agreed therein, this will apply accordingly. If a variable fee is included therein, this will apply accordingly.

The Terms and Conditions of Purchase acknowledge that transfer is not always possible in the case of third-party software. The fact that this is mentioned is merely for clarification purposes; a prohibition on transfer is usually already included in the relevant licence terms, and those terms already take precedence over other agreements. Furthermore, transfer is not possible if it is technically impossible.

Finally, it is stipulated in general terms that (in short) during the performance of the exit activities, the Agreement shall remain in force or, as the case may be, shall be extended on the same terms (Article 29.11). This is to prevent the Client from finding himself in a situation where he temporarily has no system at all (no longer the old system, but not yet the new system either). This may be the case, for example, if an unsuccessful tenderer in the new tender initiates preliminary relief proceedings (kort geding), if the content of a court ruling on the new tender leads to a reassessment or a re-tender, or if the Client has started preparations for a new tender in good time but, due to unforeseen circumstances, requires more time to complete the tender. A new Implementation may also simply require more time than initially estimated.

Here too, the situation regarding the extension of the use of third-party software has been addressed in advance.

As a general rule, all exit-related work is carried out against payment (see article 29.4 and the explanatory notes thereto). In derogation from this, article 29.11 provides that, in the event of termination due to a culpable breach, the services shall be provided free of charge. If the Agreement has been terminated due to attributable failure on the part of the Supplier, it is established that the Supplier is liable. Consequently, this provision is in effect a form of compensation in kind. The one-off destruction of data must also be carried out free of charge. This is not unreasonable, since the Supplier would have to destroy the data in any case. After all, the Supplier no longer has any grounds to retain the data after termination and could potentially be liable if the data is retained for longer.

Article 30. Applicable Law and Disputes

Article 30 stipulates that the Agreement is governed by Dutch law, that the Vienna Convention on Contracts for the International Sale of Goods does not apply, and that any disputes shall be settled by the courts in the District of the Client.

A conscious decision was made to opt for the civil courts rather than arbitration. Factors taken into account included costs and the public nature of the hearing. It is important for public bodies to be publicly accountable for the expenditure of taxpayers' money. In this context, it is not appropriate to settle disputes as a matter of course through arbitration proceedings, which are (in principle) confidential and often costly.

It is conceivable that, where appropriate, arbitration may (still) be chosen. The parties will then need to reach agreement on this – either at the time of concluding the agreement or afterwards. In particular, the specific expertise of the arbitrators may be a relevant consideration in this context.

II
Privacy,Security and Archiving

This chapter contains a number of specific articles on privacy, security and archiving. The chapter applies whenever data is processed in connection with the ICT Deliverable. This will often be the case, but certainly not always (e.g. not when selling hardware).

Article 31. Data Processor Relationship

GIBIT shall use the VNG Standard Data Processing Agreement for Clients, or, alternatively, a data processing agreement specifically agreed between the Parties. This is declared to be applicable in Article 31. The definition of 'Data Processing Agreement' (see Article 1) specifies which document is referred to.

Article 32. Information Security

Article 32 specifically concerns security. On the one hand, the article has the character of a warranty, in the sense that, pursuant to the first paragraph, the Supplier must warrant that the Client can comply with the security standard set out in the Agreement using the ICT Deliverable (paragraph 1). The manner in which the information security standards are to be met has deliberately not been specified; it is up to the Parties themselves to make agreements on this.

This article also sets out the role of the IBD as a CSIRT (paragraph 2). If the Supplier shares his contact details with the IBD, this organisation can take over all communication regarding incidents. This is beneficial for both parties: municipalities can make use of the expertise of a highly specialised organisation, and Suppliers only need to liaise with a single party regarding cybersecurity, rather than with all their customers.

On the other hand, the article also contains an obligation to the effect that, if the ICT Deliverable is managed or carried out by the Supplier, the Supplier must ensure that the ICT Deliverable actually meets that standard (paragraph 3). For practical reasons, it has been decided (in principle) to apply the same security standard as that applicable to the processing of personal data.

Paragraph 4 stipulates that the Supplier must ensure that the Personnel he engages, complies with the standards. This provision allows for the application of standards offering an equivalent level of protection, thereby providing greater flexibility for outsourcing situations. The Supplier is obliged to make backups (paragraph 5), and there is a duty to report security incidents (paragraph 6). Such an obligation already exists under the Data Processing Agreement; however, it is important for Clients to be informed about other types of security incidents as well. For the sake of clarity, the terms Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are mentioned here, as these are the terms frequently used in SLAs.

Paragraph 7 sets out the role of the IBD in more detail.

Paragraph 8 expressly stipulates that information regarding the security measures in place, is confidential. This paragraph should, of course, not be interpreted as prohibiting the Supplier from disclosing its general security measures to others, such as other clients. An exception has been made in this regard. However, the security measures implemented specifically for the Client are subject to the duty of confidentiality.

The 2025 version also takes into account the NIS2 Directive and the draft Cyber Security Act (Cyberbeveiligingswet) and Cyber Security Decree (Cyberbeveiligingsbesluit).

Article 33. Archiving

A characteristic feature of the public sector market is the obligation to comply with the Public Records Act (Archiefwet). This article therefore sets out a number of preconditions. The first paragraph stipulates that the Supplier must ensure the demonstrable management and protection of the retained data in accordance with the requirements set out in the Agreement for this purpose, such as those derived from the Municipal ICT Quality Standards. The second paragraph stipulates that the Supplier must retain data in accordance with the time limits set out in those standards. The third paragraph stipulates that the Supplier must be able to migrate the archive records to the Client's archive systems, in accordance with the Agreement (such as the Municipal ICT Quality Standards). In practice, this article may overlap to some extent with the part of the Exit scenario as described in Article 29. The fourth paragraph has been included because it is conceivable that the Supplier is the only Party that actually has the archive records in its possession. This article makes it absolutely clear that the Supplier must return such data to the Client in the event of suspension, termination or dissolution of the Agreement. The Supplier is, therefore, not allowed to 'hold those data hostage'. Here too, there is some overlap with the Exit scenario described in Article 29.

For the sake of completeness, it should be noted that the Supplier's obligation to retain records applies only for the duration of the Agreement (Article 2). The Supplier cannot (and should not) be required to retain records without an Agreement forming the basis for such retention. The Client should, however, be aware that the retention periods under the Public Records Act may be longer than the term of the Agreement. The Client must therefore take the necessary measures in good time in advance, for example by means of the Exit scenario described above or via the provisions regarding access to Data as described in Article 22, in order to ensure compliance with the Public Records Act. Once the term of the Agreement has expired, this can no longer be required of the Supplier.

For the 2025 version, the working group has examined the implications of the forthcoming amendments to the Public Records Act. The working group has concluded that the new Public Records Act does not require any substantive changes to the Terms and Conditions of Purchase.

III
Remote Services

This chapter includes a number of specific articles in the event that the ICT Deliverable (also) comprises Remote Services. The term 'Remote Services' is deliberately defined in abstract and fairly broad terms (see Article 1). It encompasses not only the services traditionally understood as 'hosting', but all remote services (such as Cloud, SaaS, etc.).

Article 34. General provision

The first paragraph sets out the obligation to make all data necessary for the provision of Remote Services, available to the Client.

If a web browser is required to use the ICT Deliverable, Article 34.2 stipulates that the ICT Deliverable must function correctly in recent and still supported versions of mainstream web browsers. In addition, the ICT Deliverable must be designed in such a way that there is no single point of failure where multiple clients are involved. This concerns cases where the application is designed in such a way that there is an automatic link between different customers. Consider, for instance, a scenario in which the same server is used for multiple clients; if one customer overloads this server, the other customers will subsequently be unable to use their application. This is in response to situations where the Supplier takes a (far too) casual approach to a truly secure and responsible design of a multi-tenant environment.

Paragraph 4 further restricts the right to suspend performance. Article 27.1 already stipulates that suspension is only permitted after a notice of default has been served. Nevertheless, the Client's dependence on the Supplier, in the case of Remote Services, is often so great that this safeguard may still prove insufficient. Invoking suspension in the context of Remote Services often amounts, in practice, to a complete disruption of the Client's business operations (as the Client would then no longer be able to access his data and/or software). That is why the standard for invoking suspension in the case of Remote Services has been tightened.

Paragraph 5 addresses the Client's own responsibility: it is up to him to keep login details confidential.

Article 35. Acceptance Procedure

The acceptance of a SaaS service differs slightly from the acceptance of other IT Deliverables. Paragraph 1 stipulates that acceptance must take place in an environment separate from the environment used for production purposes. This will also be the case in many on-premises situations; in the case of remote services, it is clear from the outset that working with separate environments is essential.

Paragraph 2 acknowledges that a test environment does not always need to be entirely comparable to the production environment. In other words: it is conceivable that the test environment might be 'lighter', provided that this does not detract from the usefulness of the Acceptance Procedure.

A key feature of Remote Services is that they are provided via the internet. It is, therefore, understandable that Suppliers are compelled to carry out certain forms of Maintenance on an ongoing basis, even during the Implementation phase. When providing services via the internet, security updates and the like will, after all, need to be installed. In practice, however, there is sometimes confusion as to whether the full maintenance phase has already begun or not. Hence the provision in the third paragraph: such Maintenance that is necessary in view of the nature of the service falls under Implementation, not under Maintenance.

Article 36. Stored Data

This article relates to the Supplier's liability for hosted data and the statutory indemnity (Article 6:196c of the Dutch Civil Code). It could be inferred from the law that the Supplier is entitled to remove hosted data promptly if a claim is made that certain information has been stored unlawfully. This article stipulates that the starting point is that the Client must first be informed of such claims (paragraph 2) and that such claims must always be discussed with the Client, unless the urgency of the matter means that such consultation cannot be awaited (paragraph 3).

Article 37. Maintenance and Availability

This article sets out certain additional provisions regarding the maintenance of the ICT Deliverable provided via Remote Services. The article stipulates a basic availability level of 98% per month on working days between 09:00 and 17:00 (paragraph 2). In all cases, these are of course basic levels; the Terms and Conditions of Purchase are, after all, designed as a safety net. In practice, different agreements regarding accessibility and availability will often be made.

Paragraph 3 stipulates that, in the case of Remote Services, the installation of Upgrades and Updates shall be carried out by the Supplier. In the context of Remote Services, this will generally be inherent to the nature of the service provision. The article should therefore be viewed primarily in conjunction with the provisions of Article 10, which specifically stated that the Client himself is, in principle, responsible for the installation (which will often not be possible in the case of Remote Services).

Paragraph 4 stipulates that, in the case of standardised Remote Services, the Client does not have the right to refuse the installation of Updates and Upgrades. This recognises that such services are generally provided in the same manner to a large number of customers and that it is therefore necessary to keep pace with developments that apply to all customers. In case an Update or Upgrade causes downtime, the Supplier shall communicate this. This could take the form of a web page providing updates on the Maintenance. In the case of urgent maintenance, this need not be done in advance, but the Supplier must keep the Client informed of developments.

Article 38. Periodic Third-Party Statement

Suppliers may be required to provide a periodic third-party statement (TPM). In practice, this is sometimes referred to as an RSO. This TPM expressly covers only the generic aspects of the service provision, not customer-specific agreements (see paragraph 2). By including this requirement, the Terms and Conditions of Purchase align with various standards and recommendations which stipulate that such a TPM is required for Remote Services. Websites such as www.isae3402.nl demonstrate that such TPMs are also common in the Netherlands. A Supplier is not required to submit both a TPM and a certification.

Article 39. Continuity Guarantees

Remote Services are subject to specific continuity risks The software provided via Remote Services and the data processed by it are, after all, located off-site. This means that in the event of the Supplier's and/or his supplier(s)'s insolvency, the Client will no longer have (unrestricted) access to his own Data, either legally or in practical terms. Article 39 acknowledges this risk and stipulates that the Parties may make additional arrangements in this regard as a preventive measure, i.e. before the actual bankruptcy situation arises(!). The article provides some examples of possible arrangements that may be made in this context. Clients are strongly advised that these arrangements are only meaningful if they are actually implemented prior to bankruptcy.

IV
Open Source

This chapter contains a number of specific articles in the event that the ICT Deliverable includes, in whole or in part, the development of Open Source software. Article 21.5 has already introduced the new principle regarding Customised Software: 'open source, unless otherwise specified'. The parties may choose not to make the Customised Software available as open source, in which case they must explicitly opt for this.

Open source is a broad concept. The working group therefore does not intend to use this chapter to regulate every aspect of the overlap between ICT procurement and open source. This chapter therefore focuses solely on situations where a Client receives Customised Software from the Supplier and wishes to make it available to others. This addresses the reality that customised software is often too expensive to develop, and/or that clients leave the intellectual property rights to customised software 'on the shelf' because they lack the capacity to make optimal use of those rights. By having Customised Software developed and subsequently publishing it as Open Source software, other municipalities will also be able to make use of this Software, and it will become cheaper to build on this Software in the future.

It is important to distinguish between the various terms used within the digital government sector in the context of open-source software: open source, open standards and Common Ground. Although these concepts are closely interrelated, they each refer to a different aspect of digital collaboration and development.

Open source refers to software whose source code is freely available. This means that public authorities can use, adapt and further develop this software without being dependent on a single supplier. It promotes transparency, encourages collaboration between organisations and enables reuse, leading to more efficient and sustainable solutions.

Open standards constitute the technical ground rules for data exchange between systems. They are publicly accessible and freely applicable specifications that ensure digital systems from different suppliers can communicate effectively with one another. The use of open standards promotes interoperability and facilitates cooperation between public authorities.

Common Ground is a collaborative programme run by Dutch public authorities aimed at jointly developing digital services. Common Ground is built on shared principles, such as open-source software, open standards and a common information architecture. This approach enables public authorities to innovate more quickly, exchange data more effectively and avoid vendor lock-in.

Article 40. General Provision

Public authorities consider it important that the Common Ground principles are followed. Paragraph 1 stipulates that it is the Supplier's responsibility to comply with these principles. Clients may ask the Supplier to explain how it applies the Common Ground principles.

Article 41. Delivery and Rights

The intellectual property rights to the open-source software shall vest in the Client. Article 41.1 explicitly states that it is the intention that the software be published as open-source software on behalf of the Client, with items such as documentation, images, build instructions and other files also being delivered.

Paragraph 2 specifies the method of acceptance: this takes place unconditionally upon publication.

Finally, paragraph 3 stipulates that the Supplier must be fully entitled and able to publish the Software. This means that no third-party intellectual property rights may prevent publication, and that no open-source software with a so-called 'viral effect' may be used. This viral effect refers to the copyleft principle found in some open-source licences. Copyleft means that when someone uses, modifies or combines existing open-source software with their own software, the new or derivative software must be made available under the same open-source licence.

There are two variants of this copyleft principle: strong copyleft (such as the GNU General Public Licence (GPL)), which requires that all software utilising GPL components be released under the same licence, and weak copyleft (such as the EUPL), which restricts this obligation to the specific components covered by that licence. Under strong copyleft, the Supplier may be obliged to disclose its own source code, which may be commercially sensitive, whereas this is not required under weak copyleft.

The purpose of paragraph 3 is to prevent the Supplier from delivering software which, due to the use of strong copyleft components or other restrictions, cannot be freely published or maintained by the client. The Supplier must, therefore, carefully check which open-source components have been incorporated into the software and ensure that the chosen licences are compatible with the obligations under the GIBIT.

Article 42. Repository

Open-source software is published on a platform such as GitHub, GitLab or Bitbucket (Article 42.1). The term 'repository' is used for this purpose. A repository is a place where the source code of an open-source project is stored, managed and shared. It is a kind of digital folder containing everything one needs to understand, use or contribute to the project.

A platform-neutral wording has been deliberately chosen; it is up to the Parties to decide between themselves which platform to choose. In any event, the Supplier shall provide a hyperlink to the final source code.

The intellectual property rights to the Software shall vest in the Client. The Supplier may not publish the Open Source software without the Client's instruction. For this reason, the repository will only be made publicly accessible after Acceptance (paragraph 2), and the Parties shall discuss how to make it public (paragraph 3). Needless to say, login details are to be treated as confidential.

Data management may form part of the IT Deliverable (paragraph 4). The Supplier is not expected to provide this service free of charge, but must be available to do so. A standard fee may be charged.

To avoid version control issues, paragraph 5 stipulates that changes must always be recorded in the repository. In this way, the public nature of the Software is safeguarded.

Article 43. Open Source License

When software is made available as open source, the terms and conditions under which this is done must be determined. Paragraph 1 stipulates that, in principle, this is done under the European Union Public Licence (EUPL). This is an open source licence developed and managed by the European Commission. This licence has been specifically designed for use by public authorities within the EU, and takes European legislation and regulations into account.

The EUPL allows software to be freely used, studied, modified and distributed. Organisations that make software available under the EUPL thereby explicitly grant others the right to reuse the source code and, if desired, to further develop it – provided they comply with the terms of the licence. Consequently, software made available under these terms, complies with the principles of the Reuse of Government Information Act (Wet hergebruik overheidsinformatie). It is possible to deviate from this, but as a rule there will often be no need to do so.

The intention is to make this available to the general public, not merely to other public authorities. It is possible that a supplier uses existing open-source software (or parts thereof), or continues to develop existing open-source software (or parts thereof). That software will already be covered by a licence. If this licence is incompatible with the EUPL, for example due to copyleft elements, it is not possible to publish the final result under the EUPL. In this case, paragraph 2 offers the option of choosing a licence other than the EUPL. This must, however, be communicated in advance, so that the client is not faced with any surprises. It is also possible in this situation to split the software, so that one part is published under the EUPL and the other part is not (paragraph 3).

Paragraph 4 stipulates, in conjunction with Article 41.3, that the Software may be made available under the chosen licence.

Article 44. Management and Maintenance

Maintenance of open-source software is also possible (Article 44.1), in accordance with the standard regime set out in Article 10. At the same time, it is recognised that maintenance for open-source software sometimes differs from that of 'standard' software, if only because (in the case of public repositories) the outside world can also participate and observe. The funding model for open source is also often different. Consequently, the Parties shall jointly determine the priorities for Corrective and Innovative Maintenance, with the Client having the deciding vote (paragraphs 2 and 3). Of course, it is not the intention that the Supplier should be required to provide this free of charge, or that the Supplier can be obliged to implement changes that degrade the software.

It is further stipulated that updates and upgrades to open-source software must also be published as open source (paragraph 4).

Article 45. Additional Financial Arrangements

Article 45 is largely self-explanatory: the provision of the Software is included in the Fee, but additional tasks are not. For example, the management and maintenance obligations (Article 44) are not free of charge.

Article 46. Termination

Article 46.1 stipulates that the early termination of the Agreement does not constitute grounds for withholding publication of the Software. No further exit is necessary (paragraph 2) because there is no vendor lock-in situation, a risk that Article 29 safeguards against.

Colophon

Author
mr. T.O. van Hoorn Dirkzwager legal & tax

Compilation and editing
mr. T Maassen, VNG Realisatie

Steering group
C.M. Pelster, Shared Service Centrum Ons
H. Schröder, gemeente Apeldoorn
H.I. Kaynak MSc., VNG Realisatie

Open Source Advice
drs. M.J.C. Hendriks, Open source expert Ministerie van Volksgezondheid, Welzijn en Sport

Vereniging van
Nederlandse Gemeenten

Nassaulaan 12
2514 JS Den Haag
+31 70 373 83 93

info@vng.nl

September 2026