VERSION 1.2 · NOVEMBER 2026

Annex to the Terms: Module descriptions

Version 1.2 · November 2026 · Replaces version 1.1 for bookings made after its publication. Change: the common part (Section 1) now describes when a configured backup recipient is alerted. For modules and add-on functions booked earlier, the version in force at booking continues to apply; Section 3.4 of the Terms applies to later changes.

This annex contains the module descriptions under Section 3.9 of the Terms for the CRA module, the NIS2 (Germany) module and the GDPR module, and the description of the contract notification clocks add-on function. The add-on function is not a module within the meaning of Section 3.9 of the Terms; it supplements booked modules. The description in force when a module or the add-on function is booked becomes part of the contract; Section 3.4 of the Terms applies to later changes.

1. Common part (applies to every module)

Legal status. In each module, the Service shows the date of the legal status its rules apply (Section 3.3a of the Terms). For the NIS2 (Germany) module and the GDPR module in this version, it is 6 October 2026.

Calculation of deadlines. Deadlines are calculated to the minute from the time the Customer records: hours and days as full 24-hour spans, months to the same calendar day and time. Deadlines are not extended over weekends or public holidays. Where a law does not count the day or hour of the event, or moves a deadline that ends on a weekend or holiday, the statutory deadline may end later than the one shown; the Service shows the earlier time. Where a law requires action "without undue delay", the deadline shown is the latest permissible time, and earlier action may be required.

Anchors. Each deadline runs from a time the Customer records, such as the time of becoming aware, the time of submission of an earlier stage or the date of a request by an authority. For cases the CRA module opens itself, Section 2 applies. The Customer records these times truthfully and without delay. A deadline cannot be calculated before its anchor is recorded.

Legal sources and reminders. Every stage names its legal source, so the Customer can check it. Reminders and target dates that do not reflect a statutory deadline are marked as such in the Service.

Drafts. Drafts follow the structure of the official form or channel named per stage. The Customer checks, completes and submits them itself through that channel. The Service has no connection to authorities' systems.

Alerts. The Service alerts the persons and channels the Customer configures, before each deadline and when it passes. Where the Customer has configured a backup recipient, the Service alerts that person as well: for CRA cases if nobody has opened or acknowledged the case two hours after its clock started, and for all other records with every reminder while nobody has taken the record on (Section 4.3 of the Terms).

Records. The Service keeps a timestamped record of each case, its stages, drafts, recorded submissions and decisions, for the booked retention period (Section 3.7 of the Terms).

Several modules. An incident recorded in the NIS2 (Germany) module or the GDPR module is one case; it opens the stages of each of these booked modules whose conditions the Customer confirms, each with its own deadline, its own recipient and its own draft. CRA module cases are kept per product (Section 2). Personal data from stages of the GDPR module are not carried into drafts of other modules.

Not included. The module does not assess whether a law applies to the Customer or whether an event reaches a legal threshold, and does not submit anything. It does not detect events in the Customer's systems; Section 2 describes when the CRA module opens a case from the sources it evaluates.

Liability. This annex describes the performance. It contains no guarantee and leaves Section 10 of the Terms unaffected.

2. CRA module

Legal rules. Regulation (EU) 2024/2847 (Cyber Resilience Act), Article 14 (1) to (4).

Cases. Each report runs in its own case per product and vulnerability or incident, in the same case list as the other modules:

- (a) an actively exploited vulnerability in a product of the Customer (Article 14 (1) and (2)). If a source the Service evaluates lists a vulnerability in a component from the Customer's SBOMs as actively exploited, the Service opens a case for the product concerned at once. The Service sets the time at which it detected the entry as the time of becoming aware; the Customer can record an earlier time, but not a later one. If the vulnerability is not contained in the product, is not actively exploited, or the product is not subject to the Regulation, the Customer can dismiss the case, stating a reason; the Customer can undo the dismissal. The Customer can also record such a case itself, for example after a notice from a security researcher, a customer or a supplier. If the same product already has an open case for the same CVE or EUVD identifier, the entry is added to that case.
- (b) a severe incident having an impact on the security of a product of the Customer (Article 14 (3) and (4)); the Customer records this case itself.

Stages, case (a) – recipient: the CSIRT designated as coordinator and ENISA, via the single reporting platform (Article 16 of the Regulation).

Stage	Anchor	Deadline	Legal source
Early warning	Becoming aware	Without undue delay, at the latest 24 hours	Article 14 (2)(a)
Vulnerability notification	Becoming aware	Without undue delay, at the latest 72 hours	Article 14 (2)(b)
Final report	Time, recorded by the Customer, from which a corrective or mitigating measure is available	At the latest 14 days after that time	Article 14 (2)(c)

Stages, case (b) – recipients as in case (a).

Stage	Anchor	Deadline	Legal source
Early warning	Becoming aware	Without undue delay, at the latest 24 hours	Article 14 (4)(a)
Incident notification	Becoming aware	Without undue delay, at the latest 72 hours	Article 14 (4)(b)
Final report	Submission of the incident notification	At the latest one month after it	Article 14 (4)(c)

Limits.

- Whether a product is subject to the Regulation, whether a vulnerability is actively exploited and whether an incident is severe is decided by the Customer (Section 3.2 of the Terms).
- Intermediate reports requested by an authority, and informing the users of the product (Article 14 (8)), are not stages of the module.
- The CRA module does not cover reporting duties under other legislation that the same incident may trigger; the NIS2 (Germany) module and the GDPR module serve that purpose.

3. NIS2 (Germany) module

Legal rules. BSI Act as amended by the NIS2 Implementation Act (BGBl. 2025 I No. 301), in particular §§ 2, 28, 32, 33, 35 BSIG; for profiles (b) to (d) §§ 5c, 5d EnWG, § 168 TKG, Articles 19a and 24 (2)(fb) of Regulation (EU) No 910/2014 (eIDAS Regulation) as amended by Regulation (EU) 2024/1183, and § 2 VDG; Directive (EU) 2022/2555 Article 23 for reference; Implementing Regulation (EU) 2024/2690 for the entity types it covers (significance criteria shown for reference, not evaluated).

Profiles. The Customer chooses one or more profiles in the module: (a) essential and important entities (§ 32 BSIG); (b) energy (§§ 5c, 5d EnWG); (c) public telecommunications networks and services (§ 168 TKG); (d) trust service providers (Articles 19a and 24 (2)(fb) eIDAS Regulation, alongside § 32 BSIG).

Scope self-check. A generic questionnaire on § 28 BSIG (sector per Annex 1 or 2, size per § 28 (1)–(4), size-independent entity types, exceptions under § 28 (5) to (7)). Exceptions under § 28 (5) lead to the energy or telecommunications profile. If the Customer states that it is a financial entity within the meaning of Article 2 (2) of Regulation (EU) 2022/2554 (§ 28 (6) BSIG), the module shows the note "Incident reporting under DORA (Art. 19) applies; this module does not cover it." and no stages under §§ 32 and 35 BSIG; the registration reminder under § 33 BSIG remains available. If the Customer states that it is gematik or a provider of services of the telematics infrastructure (§ 28 (6) no. 2 BSIG), the module shows that the BSIG's reporting duties do not apply and that the duties applying instead are not covered. The result reads "Orientation only; not a legal assessment"; the Customer decides which duties apply.

Stages, profile (a) – recipient: the joint BSI/BBK reporting office via the BSI-Portal; before registration, the online form in the reporting and information portal (MIP).

Stage	Anchor	Deadline	Legal source
Early warning	Becoming aware	Without undue delay, at the latest 24 hours	§ 32 (1) sentence 1 no. 1 BSIG
Notification	Becoming aware	Without undue delay, at the latest 72 hours	§ 32 (1) sentence 1 no. 2 BSIG
Intermediate report	BSI request	By the date the Customer records from the request	§ 32 (1) sentence 1 no. 3 BSIG
Final report	Submission of the notification (no. 2)	At the latest one month after submission of the notification; also shown: conservative target date one month after the early warning (not a statutory deadline); alerts follow the target date	§ 32 (1) sentence 1 no. 4 BSIG
Progress report	Incident still ongoing when the final-report deadline ends	At the end of the final-report deadline, with the same target date; the final report follows after handling of the incident is completed, with no statutory deadline	§ 32 (2) BSIG
Information of service recipients	BSI order	Without undue delay	§ 35 (1) BSIG
Information on significant cyber threats	Significant cyber threat; only for entities in the sectors finance, social security and basic income support for jobseekers, digital	Without undue delay; recipients: the potentially affected recipients of the	§ 35 (2) BSIG

Stage	Anchor	Deadline	Legal source
	infrastructure including managed service providers and managed security service providers, and providers of digital services, unless § 28 (5) or (6) BSIG applies	services and the BSI; the Customer makes the balancing of interests under § 35 (2) sentence 3 BSIG	
Registration	Time, recorded by the Customer, from which the entity first or again qualifies as an entity	Reminder: at the latest three months; changes without undue delay, at the latest two weeks after becoming aware of the change	§ 33 (1) and (5) BSIG

Stages, profile (b) energy – recipient: the reporting office under § 32 BSIG (BSI-Portal).

Stage	Anchor	Deadline	Legal source
Early warning	Becoming aware	Without undue delay, at the latest 24 hours	§ 5d (3) sentence 1 no. 1 EnWG
Notification	Becoming aware	Without undue delay, at the latest 72 hours, including indicators of compromise	§ 5d (3) sentence 1 no. 2 EnWG
Intermediate report	BSI request	By the date the Customer records	§ 5d (3) sentence 1 no. 3 EnWG
Final report	Submission of the notification (no. 2)	At the latest one month after submission of the notification; conservative target date and alerts as in profile (a)	§ 5d (3) sentence 1 no. 4 EnWG
Progress report and later final report	Incident still ongoing	As in profile (a)	§ 5d (3) sentence 2 EnWG with § 32 (2) BSIG

Stages, profile (c) telecommunications – recipients: Bundesnetzagentur and BSI, by e-mail with the PDF form; encryption recommended.

Stage	Anchor	Deadline	Legal source
Early warning	Becoming aware	Without undue delay, at the latest 24 hours	§ 168 (1) no. 1 TKG
Notification	Becoming aware	Without undue delay, at the latest 72 hours	§ 168 (1) no. 2 TKG
Intermediate report	Request of the Bundesnetzagentur or the BSI	By the date the Customer records	§ 168 (1) no. 3 TKG
Final report	Submission of the notification (no. 2)	At the latest one month after submission of the notification	§ 168 (1) no. 4 TKG
Progress report; final report after completion of handling	Incident still ongoing	At the end of the final-report deadline; then within one month after completion of handling	§ 168 (2) TKG
Detailed report	Demand of the Bundesnetzagentur	By the date the Customer records	§ 168 (4) sentence 2 TKG
Public information	Order of the Bundesnetzagentur	As ordered	§ 168 (6) sentence 2 TKG
Information of potentially affected users	Particular and significant risk of a security incident	No statutory deadline; shown as a task without a deadline	§ 168 (7) TKG

Stages, profile (d) trust services – recipients: the supervisory body (the BSI for certificates for website authentication, the Bundesnetzagentur for the other trust services; § 2 (1) VDG), identifiable affected individuals and the public (non-qualified providers: if it is of public interest; qualified providers: at the request of the supervisory body). The channel is recorded by the Customer. If the incident is also a significant incident, the stages of profile (a) apply in addition, because trust service providers are entities under § 28 BSIG; if it affects personal data, Articles 33 and 34 GDPR apply in addition, which the GDPR module covers where booked. These reports are made separately; no authority is assumed to forward them.

Stage	Anchor	Deadline	Legal source
Notification (non-qualified provider)	Becoming aware	Without undue delay, at the latest 24 hours	Article 19a (1)(b) eIDAS Regulation
Notification (qualified provider)	Occurrence of the incident	Without undue delay, at the latest 24 hours after occurrence; while the time of occurrence is not recorded, the Service shows the deadline from becoming aware only provisionally, with the note "The 24-hour period runs from the incident, not from awareness. Record the time of the incident; until then the date shown is provisional and may be later than the legal deadline.", and alerts all configured recipients at once	Article 24 (2)(fb) eIDAS Regulation
Public information (qualified provider)	Request of the supervisory body	As requested	Article 24 (2)(fb) eIDAS Regulation

Free-text fields of this profile carry the hint: "Name no individual person."

Limits.

- This module covers Germany only; other Member States are not covered.
- The Service has no connection to the BSI-Portal or other reporting channels; the module keeps its own copy of the Customer's drafts and recorded submissions.
- Registration itself (§ 33 BSIG) is done by the Customer in the BSI-Portal; the login uses "Mein Unternehmenskonto" with an ELSTER organisation certificate.
- The module does not assess whether a security incident is significant; the criteria are shown for reference.

4. GDPR module (personal data breaches)

Legal rules. GDPR Articles 4 (12), 33 and 34; BDSG § 29 (1) and §§ 42 (4), 43 (4) (shown as notes); § 169 TKG with Regulation (EU) No 611/2013 (telecommunications profile).

Modes. The module includes both modes in every size; the Customer chooses the mode per case.

Controller (the Customer is the controller):

Stage	Anchor	Deadline	Legal source
Notification to the competent supervisory authority	Becoming aware	Without undue delay and, where feasible, within 72 hours, unless the breach is unlikely to result in a risk; if later, with a field for the reasons for the delay (Article 33 (1) sentence 2 GDPR)	Article 33 (1) GDPR
Content	–	Nature of the breach with categories and approximate number of data subjects and records; contact point; likely consequences; measures	Article 33 (3) GDPR
Supplements	Earlier submission	Without undue further delay; reminder after 14 days (BitHive default; no legal or authority deadline)	Article 33 (4) GDPR
Communication to data subjects	Customer's decision that there is a high risk	Without undue delay; reminders after 24 and 72 hours (not statutory deadlines); exceptions under Article 34 (3) GDPR as a checklist; under the exception in Article 34 (3)(c) GDPR, a public communication takes the place of the communication to data subjects; confidentiality exception under § 29 (1) BDSG as a note	Article 34 (1) and (2) GDPR
Communication ordered by the supervisory authority	Order	As ordered	Article 34 (4) GDPR
Documentation	Every breach, including those not notified	Ongoing	Article 33 (5) GDPR

The module shows the channel of the supervisory authority the Customer has recorded as competent for the entity concerned (the authority of the German Land or the BfDI), where the Service holds a channel for that authority. Where it holds none, the Customer takes the channel from the authority's website.

Processor (the Customer processes personal data on behalf of its own customers):

Stage	Anchor	Deadline	Legal source
Notification to each affected controller	Becoming aware	Without undue delay; reminders after 24 and 72 hours (not statutory deadlines)	Article 33 (2) GDPR

The module drafts the notification with the information under Article 33 (3) GDPR that the controller needs, and records when each controller was informed. The Customer's controllers decide on notifying the supervisory authority and data subjects. Shorter deadlines from the Customer's contracts with its controllers are recorded by the Customer with the contract notification clocks add-on function (Section 5).

Telecommunications profile (providers of publicly available telecommunications services):

Stage	Anchor	Deadline	Legal source
First notification to the Bundesnetzagentur and the BfDI	Detection	Without undue delay, where feasible within 24 hours	§ 169 (1) sentence 1 TKG; Article 2 (2) Regulation (EU) No 611/2013
Second notification	First notification	At the latest three days later	Article 2 (3) first subparagraph Regulation (EU) No 611/2013
Remaining information	Second notification	As soon as possible, with reasons	Article 2 (3) second subparagraph Regulation (EU) No 611/2013
Notification of subscribers and affected individuals	Detection	Without undue delay, whether or not the authorities have been notified; as a decision aid, both thresholds: likely to adversely affect (Article 3 (1) of the Regulation) and seriously impaired (§ 169 (1) sentence 2 TKG); exception for unintelligible data as a checklist	§ 169 (1) sentences 2 and 3 TKG; Articles 3, 4 Regulation (EU) No 611/2013
Notification ordered by the Bundesnetzagentur	Order	As ordered	§ 169 (1) sentence 4 TKG
Inventory of breaches	Every breach	Ongoing	§ 169 (3) TKG

Data minimisation. The module records categories and approximate numbers of data subjects and records, not their identities. Free-text fields carry the hint: "Name no individual person."

Limits.

- The module does not assess the risk to data subjects; the risk questions are a checklist the Customer answers.
- The Customer records which supervisory authority is competent for each entity; the module does not determine it. Cross-border cases with a lead supervisory authority (Article 56 GDPR) are shown as a note, not resolved.
- Channels are stored only for German supervisory authorities. For other Member States the stages of Article 33 GDPR apply, and the Customer records the channel.

5. Contract notification clocks (add-on function)

Content. The Customer records notification duties from its own contracts, for example clauses in data processing agreements, service level agreements or customer and supplier contracts that require notice of an incident within a set time, including clauses agreed with customers in the financial sector. In the Service, a contract is one entry recorded under Contracts, and it holds one notification duty. For each contract, the Customer records:

- the counterparty;
- the clause as written, including the event that triggers the duty, and where the clause is found;
- the moment from which the period runs, chosen from those the Service offers: when the Customer becomes aware of the incident, when the incident occurred, or the event the contract names;
- the period, where the contract sets one;
- optionally, a business address for notices.

Where a contract contains several notification duties, for example a first notice and a full report, the Customer records each duty as a separate contract.

When the Customer states on an incident record that the incident triggers a contract's notification duty, the Service opens that duty, calculates its deadline where a period is recorded, sends alerts and reminders, drafts the notice with the fields the Service provides, and records the notice when the Customer marks it as sent, with its time, channel, recipient and a copy. The Customer completes the draft and sends the notice itself, through the channel its contract names. Section 1 (Common part) applies accordingly, with these differences: each duty names the contract it comes from instead of a legal source; drafts follow the fields described above instead of an official form; "Legal status" and "Several modules" do not apply.

Start of the period. If the contract runs the period neither from awareness nor from the occurrence of the incident, the Customer chooses "the event the contract names" and records its time. Until that time is recorded, the Service calculates no deadline and sends no reminders.

Periods. Periods are recorded in hours, days, weeks or months, up to ten years. Deadlines are calculated under Section 1 (Calculation of deadlines): from the recorded time, hours exactly, a day as 24 hours, a week as seven times 24 hours, a month to the same calendar day and time in the month in which the period ends or, where that month has no such day, to its last day; without extension over weekends or public holidays. Where a contract counts in business days or in another unit, the Customer records the shortest period in the units above that the contractual period can amount to.

Contracts without a period. If the Customer records no period, the Service calculates no deadline. It sends reminders 24 and 72 hours after the recorded moment; they are marked as reminders and do not reflect a deadline (Section 1, Legal sources and reminders).

Notifications to controllers. A processor's notification to the controller under Article 33 (2) GDPR is a stage of the GDPR module (Section 4). With the add-on function booked, the Customer can record, for a contract with a controller, the period and the moment its contract sets for that notification; the GDPR module's stage then uses that period (Section 4). Contracts with controllers do not count towards the size of the add-on function, with or without such a period.

Size. The add-on function is an option within the meaning of Section 3.7 of the Terms. It is booked in a size measured in contracts. The price list states the sizes and their prices, the module sizes with which each size can be booked, and the number of contracts above which the add-on function is available only by offer (Section 2.3 of the Terms). In an Enterprise plan, the offer states the size. Each contract recorded for the add-on function counts once; contracts with controllers (above) and archived contracts do not count (Section 3.6a (a) of the Terms). A contract with an open notification duty cannot be archived. An archived contract cannot be named in an incident record until it is restored; once restored, it counts again. Section 3.6a (c) and (d) of the Terms applies. Discounts on modules, in particular the bundle discount (Section 7.1a of the Terms) and promotion codes (Section 7.7 of the Terms), do not apply to the add-on function.

Changes. Section 7.6 of the Terms applies to booking, enlarging, reducing and removing the add-on function, with these rules:

- A smaller size is possible only if the contracts in use fit it; the Customer archives excess contracts first. If, when the change is due to take effect, the contracts in use no longer fit the smaller size, the change is not applied and the booked size continues; BitHive informs the Customer. The last sentence of Section 7.6 (e) of the Terms does not apply in this case.
- If a change to the modules would leave no module in a size with which the booked size can be booked, the add-on function must be changed in the same change to a size that can be booked with the remaining modules, or removed.

- A removal takes effect at the end of the billing period; during the free trial, it takes effect at once. From then on, no new notification duties are opened under the Customer's contracts. Notification duties that are open at that moment keep their deadlines and alerts until the Customer closes them, as Section 7.6 (c) of the Terms provides for modules. The contracts and their records remain available for export within the booked retention period. For notifications to controllers, deadlines already calculated from a contractual period stay; deadlines calculated after the removal takes effect follow Article 33 (2) GDPR only (Section 4). Before the Customer confirms the removal, the Service points this out.

Limits.

- BitHive does not read, interpret or check the Customer's contracts. The duties apply exactly as the Customer records them. The Customer decides whether an incident triggers a duty under a contract; Section 3.2 of the Terms applies accordingly.
- The Service sends nothing to the Customer's counterparties. Alerts and reminders go only to the contacts and channels the Customer has set up.
- The add-on function does not make BitHive a party to the Customer's contracts, including contracts with financial entities; BitHive takes on no obligation that the Customer owes its counterparties.

Download as PDF·All legal documents