SAMPLE: CONSOLIDATED GDPR COMPLIANCE REPORT

Regulation (EU) 2016/679

Verdigris Goods Limited

> **SAMPLE.** Verdigris Goods Limited is an example company, used out of respect for the privacy of the businesses that use this system. Every name, number, finding and date in this document is illustrative.

Report assembled: 23 September 2026
Prepared using: compliancesme.com
Instrument: A-001, Regulation (EU) 2016/679
Working files completed: 10 of 10
Entity-facing obligations covered: 95

TABLE OF CONTENTS

1. ENTITY IDENTIFICATION

Field	Detail
Entity name	Verdigris Goods Limited
Registration number	9999999 (Companies Registration Office, Ireland)
Legal form	Private company limited by shares
Sector	Online retail of physical goods: homeware and small electrical accessories
Member State	Ireland
Establishments	One: Unit 7, Ardilaun Business Park, Dublin 12, Ireland, comprising the registered office and the single warehouse
Supervisory authority	Data Protection Commission, Ireland
Data Protection Officer	Not designated. No ground under Article 37(1) applies (see section 12.1)
DPO contact details	Not applicable. Data protection enquiries are handled by Aoife Brennan, Operations Manager, privacy@verdigris.example
GDPR territorial basis	Establishment in the Union. The entity is a controller established in Ireland and processes personal data in the context of that establishment (Article 3(1))
Role	Controller for every processing activity assessed. The entity acts as a processor for no other controller
Employees	12 headcount, 11.4 full-time equivalent

Field	Detail
Annual turnover	EUR 4,200,000 for the year ended 31 December 2025
Data processing activities summary	Thirteen recorded activities covering customer accounts, order fulfilment, payment and fraud screening, customer service including an AI assistant, marketing email, website analytics, returns and warranty handling, accounting records, employee administration and payroll, sickness absence records, recruitment, warehouse CCTV, and supplier contact management. Customers are consumers in Ireland, Germany, France, the Netherlands, Belgium, Spain and the United Kingdom

2. EXECUTIVE SUMMARY

Overall compliance status: PARTIALLY COMPLIANT

Verdigris Goods Limited holds the core of a working data protection framework. It maintains a record of processing activities, a lawful basis for every one of its thirteen processing activities, written agreements with all six of its processors, a breach response procedure that has been used twice, and a request-handling process that has met the one-month deadline of Article 12(3) on every request received. Of the 95 entity-facing obligations under Regulation (EU) 2016/679, 43 are assessed as COMPLIANT, 25 as PARTIAL and 27 as NOT APPLICABLE on a recorded ground. No obligation is assessed as NON-COMPLIANT and none is left unassessed.

Twenty-five gaps were identified. Three are HIGH. The highest-severity gap is the absence of a data protection impact assessment for the customer service assistant deployed on 7 April 2026, which Article 35(1) requires to be carried out prior to the processing. The two further HIGH gaps concern the same vendor relationship: the agreement with the assistant vendor omits two of the eight mandatory processor clauses required by Article 28(3), and the transfer of customer service transcripts to a sub-processor in the United States relies on standard contractual clauses without a transfer impact assessment under Article 46(1).

The recommended priority action is to complete the data protection impact assessment for the customer service assistant, and to suspend or restrict the assistant's processing of transcripts until that assessment is signed off. The same piece of work will close the two remaining HIGH gaps, because the impact assessment identifies the contractual and transfer defects that the vendor agreement must be amended to fix.

Metric	Value
Total entity-facing obligations	95
Obligations assessed as COMPLIANT	43
Obligations assessed as PARTIAL	25
Obligations assessed as NOT APPLICABLE	27
Obligations assessed as CONCERN	0
Obligations assessed as NON-COMPLIANT	0
Obligations assessed as NOT ASSESSED	0
Obligations assessed as NOT SUBMITTED	0
Total gaps identified	25
CRITICAL gaps	0
HIGH gaps	3
MEDIUM gaps	19
LOW gaps	3

3. LAWFULNESS, FAIRNESS AND PROCESSING PRINCIPLES

3.1 Processing Principles

OB-004, Recital 74: Accountability measures

STATUS: COMPLIANT

The entity holds a Data Protection Policy dated 12 January 2026, a processing activity register, a processor register, a breach register, a retention schedule and signed training records for all 12 staff. Recital 74 requires the controller to implement appropriate and effective measures and to be able to demonstrate compliance of processing activities with the Regulation, including the effectiveness of those measures. The Managing Director reviews the policy set annually and reviewed it on 12 January 2026. Measures are scaled to a 12-person retailer with one warehouse and one hosting environment.

OB-013, Recital 39: Time limits for erasure and periodic review

STATUS: PARTIAL

A retention schedule dated 12 January 2026 sets a period and a criterion for eleven of the thirteen recorded processing activities. No time limit is set for website analytics data or for the records of unsuccessful job applicants, and no periodic review of either category is scheduled. Recital 39 requires the controller to establish time limits for erasure or for periodic review. Gap GAP-04 refers.

OB-016, Article 5(1): Principles relating to processing

STATUS: PARTIAL

Article 5(1) requires the controller to process personal data lawfully, fairly and transparently, to collect for specified, explicit and legitimate purposes and not further process incompatibly, to ensure data are adequate, relevant and limited to what is necessary, to ensure data are accurate and kept up to date, to keep data in identifiable form no longer than necessary, and to process with appropriate security.

Lawfulness, fairness and transparency (Article 5(1)(a)): satisfied. Each activity carries a recorded lawful basis, a published privacy notice covers every direct collection channel, and the two indirect sources without one are recorded at GAP-09. Fairness is assessed at the point a new activity is added, using a four-question check recorded in the Data Protection Policy.

Purpose limitation (Article 5(1)(b)): satisfied. Purposes are recorded in the processing activity register before collection begins and the register names the Operations Manager as owner. No further processing for a new purpose has taken place since 25 May 2018.

Data minimisation (Article 5(1)(c)): satisfied. The checkout form was reduced in February 2026 from fourteen fields to nine, removing date of birth, gender and a free-text profile field. The last holdings review was completed on 20 February 2026.

Accuracy (Article 5(1)(d)): satisfied. Customers may correct their own address, email and telephone number in the account area. Bounced email addresses are flagged within 24 hours and suppressed after three consecutive failures.

Storage limitation (Article 5(1)(e)): not satisfied. The retention schedule sets 36 months from last sign-in for dormant customer accounts, and that period is not enforced. At the date of assessment the platform holds 7,412 accounts with no sign-in for more than 36 months. Gap GAP-05 refers.

Integrity and confidentiality (Article 5(1)(f)): satisfied. Transport encryption on all customer-facing services, encryption at rest on the hosted database and backups, role-based access with least privilege, multi-factor authentication for all 12 staff accounts, and daily backups held for 35 days.

OB-017, Article 5(2): Accountability principle

STATUS: COMPLIANT

Article 5(2) requires the controller to be responsible for, and to be able to demonstrate compliance with, Article 5(1). The entity produced the policy set, the registers, the retention schedule, the training records and this assessment on request during the session. The Managing Director signs the annual review. This obligation is assessed as satisfied notwithstanding the storage limitation gap recorded at OB-016, because the entity identified, documented and quantified that gap rather than asserting compliance.

RETENTION SCHEDULE

Data category	Retention period	Criterion	Enforced
Customer account records	36 months from last sign-in	Dormancy	No (GAP-05)
Order and delivery records	Six years from the end of the financial year	Tax and company law record-keeping, provision not cited (GAP-06)	Yes
Payment authorisation records	Six years from the end of the financial year	Tax and company law record-keeping, provision not cited (GAP-06)	Yes
Fraud screening outcomes	24 months from the transaction	Period over which repeat patterns are reviewed	Yes
Customer service transcripts	24 months from case closure	Warranty and complaint window	Yes
Marketing subscriber records	24 months from last engagement	Inactivity	Yes
Marketing suppression list	Retained indefinitely	Necessary to honour objections under Article 21(3)	Yes
Website analytics data	Not stated	Not stated (GAP-04)	No
Returns and warranty records	Six years from the end of the financial year	Tax and company law record-keeping, provision not cited (GAP-06)	Yes
Accounting and statutory records	Six years from the end of the financial year	Tax and company law record-keeping, provision not cited (GAP-06)	Yes
Employee records	Six years after employment ends	Limitation period for employment claims	Yes

Data category	Retention period	Criterion	Enforced
Sickness absence records	Three years after the absence ends	Employment administration	Yes
Unsuccessful applicant records	Not stated	Not stated (GAP-04)	No
Warehouse CCTV footage	30 days	Incident review window	Yes, automatic overwrite
Supplier contact records	Duration of the relationship plus two years	Business continuity	Yes

3.2 Accountability

OB-051, Article 24(1): Controller responsibility

STATUS: COMPLIANT

Article 24(1) requires the controller to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation, and to review and update those measures where necessary. The measures are set out in the Data Protection Policy and the Information Security Standard, both dated 12 January 2026. The February 2026 checkout field reduction is the recorded example of a risk profile driving a specific measure: collecting fewer identifying fields reduced the consequence of any compromise of the order database. The last full review was the annual review of 12 January 2026, triggered by the review cycle.

OB-052, Article 24(2): Data protection policies

STATUS: COMPLIANT

Article 24(2) requires appropriate data protection policies where proportionate in relation to the processing activities. The entity holds four written policies: the Data Protection Policy, the Information Security Standard, the Data Subject Request Procedure and the Breach Response Procedure. Each was reviewed on 12 January 2026 and approved by the Managing Director. Staff complete data protection training at induction and annually, and the 2026 round was completed by all 12 staff by 6 February 2026.

3.3 Lawful Basis

OB-018, Article 6(1): Lawfulness of processing

STATUS: PARTIAL

Article 6(1) requires processing to rest on at least one of six lawful bases: consent, contract performance, legal obligation, vital interests, public interest or official authority, or legitimate interests. Every one of the thirteen recorded activities carries a lawful basis and the basis is held in the same register as the record of processing activities, not in a separate list. Two legitimate interests assessments are on file, for fraud screening and for warehouse CCTV, each recording the interest pursued, the necessity of the processing and the balancing against the rights and freedoms of data subjects. The gap is that for the four activities relying on Article 6(1)(c), the register names "Irish tax and company law" without citing the provision that imposes the obligation. Gap GAP-06 refers.

LAWFUL BASIS REGISTER

Processing activity	Lawful basis, Article 6(1)	Justification
A1 Customer accounts	Article 6(1)(b) contract	The account is the means by which the customer places and tracks orders, and is requested by the customer
A2 Order processing and fulfilment	Article 6(1)(b) contract	Processing is necessary to supply and deliver the goods ordered
A3 Payment processing	Article 6(1)(b) contract	Processing is necessary to take payment for the order
A3 Fraud screening	Article 6(1)(f) legitimate interests	Interest: preventing payment fraud and chargeback loss. Necessity: card-not-present orders cannot be screened by other means. Balance: screening outputs are advisory, a person reviews every refusal, and no order is refused by automated means alone. Assessment dated 3 February 2026
A4 Customer service enquiries	Article 6(1)(b) contract	Handling enquiries about orders placed is part of supplying the goods
A4 Customer service quality review	Article 6(1)(f) legitimate interests	Interest: accuracy of replies drafted by the assistant. Necessity: a sample of transcripts must be read to verify quality. Balance: sampling is limited to 2 per cent of cases and reviewers see order data only. Assessment dated 3 February 2026
A5 Marketing email	Article 6(1)(a) consent	Consent is requested separately at checkout and at newsletter sign-up, and can be withdrawn in one action

Processing activity	Lawful basis, Article 6(1)	Justification
A6 Website analytics and cookies	Article 6(1)(a) consent	Non-essential cookies and analytics identifiers are set only after the visitor accepts them in the banner
A7 Returns, refunds and warranty	Article 6(1)(b) contract and Article 6(1)(c) legal obligation	Returns handling performs the contract; the refund record is kept to meet statutory record-keeping (provision not cited, GAP-06)
A8 Accounting and statutory records	Article 6(1)(c) legal obligation	Statutory record-keeping (provision not cited, GAP-06)
A9 Employee administration and payroll	Article 6(1)(b) contract and Article 6(1)(c) legal obligation	The contract of employment, and payroll withholding and reporting duties (provision not cited, GAP-06)
A10 Sickness absence records	Article 6(1)(b) contract and Article 6(1)(c) legal obligation, with Article 9(2)(b) for the health data	Absence administration under the contract of employment and employment law (provision not cited, GAP-06 and GAP-07)
A11 Recruitment, successful candidate	Article 6(1)(b) contract	Steps taken at the request of the data subject prior to entering a contract
A11 Recruitment, unsuccessful applicants	Article 6(1)(f) legitimate interests	Interest: defending a claim about the selection decision. Necessity: interview notes are the only record of the decision. Balance: applicants are told at application. Assessment dated 3 February 2026
A12 Warehouse CCTV	Article 6(1)(f) legitimate interests	Interest: stock loss and access control at a single unstaffed-at-night warehouse. Necessity: four cameras cover the loading bay and stock cage only, not rest areas. Balance: signage at both entrances, 30-day overwrite. Assessment dated 3 February 2026
A13 Supplier contact management	Article 6(1)(f) legitimate interests	Interest: managing supply relationships. Necessity: business contact details are required to place and chase orders. Balance: business contact data only. Assessment dated 3 February 2026

No activity relies on consent where contract performance or legitimate interests would be the correct basis. Marketing email is the only customer-facing activity on consent, and it is not a condition of any purchase. The entity is not a public authority and relies on no ground under Article 6(1)(e).

3.4 Special Category and Criminal Data

OB-024, Article 9(1): Special category data prohibition

STATUS: PARTIAL

Article 9(1) prohibits the processing of special categories of personal data unless an exception under Article 9(2) applies. The entity processes one special category: data concerning health, in the form of medical certificates and fitness-to-work statements held for sickness absence administration, affecting up to 12 data subjects. It relies on Article 9(2)(b), employment and social security law. The gap is the one the practical guidance for this file names as the most frequent error: the entity has not identified the specific Member State law that authorises the processing and has not recorded the appropriate safeguards for the fundamental rights and interests of the data subjects. Gap GAP-07 refers.

Data category	Processed	Article 9(2) exception	Safeguards
Racial or ethnic origin	No	Not applicable	Not applicable
Political opinions	No	Not applicable	Not applicable
Religious or philosophical beliefs	No	Not applicable	Not applicable
Trade union membership	No	Not applicable	Not applicable
Genetic data	No	Not applicable	Not applicable
Biometric data for unique identification	No	Not applicable	Not applicable
Data concerning health	Yes, sickness absence records	Article 9(2)(b) asserted, Member State law not identified (GAP-07)	Paper certificates held in a locked cabinet, digital copies restricted to the Managing Director and the Operations Manager. No further safeguards documented

Data category	Processed	Article 9(2) exception	Safeguards
Data concerning sex life or sexual orientation	No	Not applicable	Not applicable

No processing relies on explicit consent under Article 9(2)(a), so no separate explicit consent mechanism is required.

OB-025, Article 10: Criminal conviction data

STATUS: NOT APPLICABLE

The entity processes no personal data relating to criminal convictions and offences or related security measures, and maintains no register of criminal convictions. Recruitment does not include criminal record checks for any of the roles it hires. Ground: the processing described in Article 10 is not carried out.

3.5 Identification Exemption

OB-026, Article 11(1): Processing not requiring identification

STATUS: COMPLIANT

Article 11(1) provides that where the purposes do not require identification of a data subject, the controller is not obliged to maintain, acquire or process additional information in order to identify the data subject solely to comply with the Regulation. The entity reviewed its activities and identified one where identification is not required: website analytics, which uses a pseudonymous identifier and a truncated IP address and is not joined to the account database. The entity does not acquire or keep any additional information to re-identify analytics records, and its privacy notice tells visitors that analytics requests cannot be answered by identity alone.

4. CONSENT MANAGEMENT

4.1 Conditions for Consent

OB-014, Recital 42: Consent requirements

STATUS: COMPLIANT

Recital 42 requires the controller to be able to demonstrate that the data subject has given consent, and requires consent declarations to be provided in an intelligible and easily accessible form, using clear and plain language and without unfair terms. Consent is captured in two places: an unticked box at checkout and a newsletter sign-up form. Both use a clear affirmative act. No pre-ticked box, silence or inactivity is treated as consent anywhere on the site. The declaration is 38 words, written in plain English and reviewed against the unfair terms test in Council Directive 93/13/EEC by the entity's solicitor on 19 January 2026. Consent is separate for marketing email and for non-essential cookies, so consent is specific to each purpose. Service is never conditional on marketing consent.

OB-019, Article 7(1): Demonstrating consent

STATUS: PARTIAL

Article 7(1) requires the controller, where processing is based on consent, to be able to demonstrate that the data subject has consented. The marketing platform holds a record for each of the 18,200 subscribers showing who consented, the date and time, the channel and the IP address. For sign-ups after 1 March 2024 the record also stores the exact wording shown at the moment of consent. For the 6,050 subscribers who signed up before that date the wording is not stored, so the entity can show that consent was given but cannot show what the subscriber was told. Gap GAP-08 refers. Consent records are kept for 24 months after withdrawal, to evidence the lawfulness of processing before withdrawal.

OB-020, Article 7(2): Consent request presentation

STATUS: COMPLIANT

Article 7(2) requires that where consent is given in a written declaration which also concerns other matters, the request for consent is presented in a manner clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Consent language appears in one mixed document, the checkout page, alongside the terms of sale. It sits in its own bordered block below the payment section, under its own heading, with the box unticked. The block was reviewed on 19 January 2026 by the Operations Manager and the solicitor, and the review moved the consent block out of the terms acceptance line, where it had previously been bundled.

OB-021, Article 7(3): Right to withdraw consent

STATUS: COMPLIANT

Article 7(3) requires that the data subject can withdraw consent at any time, that withdrawal is as easy as giving it, and that the data subject is informed of the right before giving consent. Consent is given by one click on a box; it is withdrawn by one click on the unsubscribe link in every marketing email, or by one switch in the account preference centre. Cookie consent is withdrawn by one click in the footer preferences link. The text shown immediately above the checkout consent box reads: "You can withdraw this consent at any time by clicking unsubscribe in any email or changing your preferences in your account. Withdrawal does not affect anything we sent before." Withdrawal takes effect on the

next send cycle, within 24 hours, and the subscriber receives a confirmation. Withdrawals are recorded in the same platform as the original consent, with date, channel and the activities affected.

4.2 Child's Consent

OB-022, Article 8(1): Child's consent for information society services

> STATUS: NOT APPLICABLE

The entity offers an online shop, which is an information society service, but does not offer it directly to children. The terms of sale require the purchaser to be 18 or over, the product range is homeware and small electrical accessories, the site carries no content directed at children, and a review of the marketing creative and the age composition of the subscriber list was completed on 2 February 2026 and recorded. Ground: no information society service is offered directly to a child, so the Article 8(1) condition does not arise.

OB-023, Article 8(2): Age verification

> STATUS: NOT APPLICABLE

Ground: Article 8(2) applies only where consent is given or authorised by the holder of parental responsibility under Article 8(1). No such consent is sought, so the verification duty does not arise.

5. TRANSPARENCY AND INFORMATION PROVISION

DATA COLLECTION CHANNEL MAP

Direct channel	Personal data collected	Privacy notice in place	Last updated
Website account registration	Name, email, password, telephone	Yes	12 January 2026
Website checkout	Delivery and billing address, order lines, payment token	Yes	12 January 2026
Newsletter sign-up form	Name, email	Yes	12 January 2026
Customer service email and web form	Name, email, order reference, enquiry content	Yes	12 January 2026
Cookies and website analytics	Pseudonymous identifier, pages viewed, device type, truncated IP address	Yes, cookie notice	12 January 2026
Returns portal	Name, order reference, reason for return, bank details where required	Yes	12 January 2026
Warehouse CCTV	Images of people at the loading bay and stock cage	Yes, signage at both entrances	4 February 2026
Recruitment applications by email	CV, contact details, interview notes	Yes, applicant notice	12 January 2026
Employee onboarding	Name, address, PPS number, bank details, tax details	Yes, staff privacy notice	12 January 2026

Indirect source	Categories obtained	Purpose	Privacy notice in place	Last updated
Corrib Logistics Limited and Rheinpost Parcel GmbH	Delivery status, signature confirmation, redirect and safe-place instructions given by the customer to the courier	Completing delivery and answering delivery enquiries	No	Not applicable
Pactum Payments Limited	Authorisation result, fraud score, chargeback notices	Taking payment and screening fraud	No	Not applicable

Channel or source	Gap description
Courier delivery data	No Article 14 notice covers personal data the couriers pass back to the entity
Payment provider outcome data	No Article 14 notice covers fraud scores and chargeback data received from the payment provider

5.1 Transparent Communication

OB-002, Recital 60: Transparency principle

STATUS: COMPLIANT

Recital 60 requires the controller to provide the data subject with information on the existence and purposes of the processing operation, on profiling and its consequences, on whether the provision of personal data is obligatory and on the consequences of not providing it. The privacy notice is linked from the footer of every page, from the account area and from the checkout consent block, and a short summary appears at each collection point. The entity carries out no profiling within the meaning of Article 4(4): the fraud score is produced for a single transaction and is not used to evaluate personal aspects of the customer, and the marketing platform sends the same content to the whole list. That verification was carried out on 2 February 2026 and recorded.

OB-027, Article 12(1): Transparent information and communication

STATUS: COMPLIANT

Article 12(1) requires the controller to take appropriate measures to provide the information under Articles 13 and 14 and the communications under Articles 15 to 22 and 34 "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". The notice is 1,340 words, written at a reading level checked with a readability tool in January 2026, and is structured under nine question headings. It is published in English, German, French, Dutch and Spanish, matching the five languages in which the shop sells. No data subjects are children, so no child-adapted version is required. The notice was last reviewed on 12 January 2026 as part of the annual review.

5.2 Information at Collection

OB-032, Article 13(1): Information where data are collected from the data subject

STATUS: COMPLIANT

The notice names Verdigris Goods Limited, its registered address, its telephone number and the privacy contact address. It states that no data protection officer is designated and gives the contact point instead. It lists each purpose with its lawful basis, and names the legitimate interests pursued for fraud screening, quality review, recruitment, CCTV and supplier contacts. It lists the categories of recipients: the hosting provider, the marketing platform, the analytics provider, the customer service assistant vendor, the payroll provider, the accountant, the payment provider and the couriers. It states that one transfer is made to the United States by a sub-processor of the customer service assistant vendor and that standard contractual clauses under Article 46(2)(c) are in place, and it says how to request a copy of them.

OB-033, Article 13(2): Additional information at collection

STATUS: PARTIAL

The notice gives the storage period or the criterion for each category, lists all six rights under Articles 15 to 21, states the right to withdraw consent and that withdrawal does not affect prior processing, names the Data Protection Commission as the authority to which a complaint may be made, and states that no automated decision-making within Article 22(1) takes place. One item required by Article 13(2) is missing: the notice does not say whether the provision of personal data is a contractual requirement or a requirement necessary to enter into a contract, nor what happens if the customer does not provide it. Gap GAP-23 refers.

OB-034, Article 13(3): Further processing notification

STATUS: COMPLIANT

Article 13(3) requires the controller, where it intends to further process personal data for a purpose other than that for which they were collected, to provide the data subject with information on that other purpose before the further processing. The entity has carried out no further processing for a new purpose since 25 May 2018. The Data Protection Policy sets the test: any proposal to use existing data for a new purpose goes to the Operations Manager, who records a compatibility assessment against Article 6(4) and, where the purpose is new, requires notification to the customer before processing starts. The template for that assessment is held with the policy.

5.3 Information for Indirect Collection

OB-035, Article 14(1) to (2): Information where data are not obtained from the data subject

STATUS: PARTIAL

The entity obtains personal data from two indirect sources: delivery instructions and signature confirmations passed back by the two couriers, and authorisation results, fraud scores and chargeback notices received from the payment provider. Neither source is covered by an Article 14 notice. The published privacy notice describes data flowing out to these recipients but not data flowing back in, so it does not give the categories of personal data concerned, the source of the data, or the storage period for the data received. Gap GAP-09 refers. The entity relies on no exemption under Article 14(5).

OB-036, Article 14(3): Timing of the indirect collection notice

STATUS: PARTIAL

Article 14(3) requires the information to be provided within a reasonable period after obtaining the data and at the latest within one month, or at the time of first communication with the data subject, or when the data are first disclosed to another recipient, whichever is earliest. Because no Article 14 notice exists for either source, no timing can be evidenced and no timestamped records are kept. Gap GAP-10 refers.

OB-037, Article 14(4): Further processing of indirectly obtained data

STATUS: COMPLIANT

Article 14(4) requires the controller, where it intends to further process indirectly obtained data for a new purpose, to provide the data subject with information on that purpose before the further processing. Delivery confirmations and payment outcomes are used only for the purpose for which they are received, that is completing the order and screening fraud. No further processing for another purpose has occurred and the same compatibility assessment procedure recorded at OB-034 governs any proposal to introduce one.

5.4 Right to Object Notice

OB-048, Article 21(4): Right to object notice at first communication

STATUS: PARTIAL

Article 21(4) requires the right to object to be explicitly brought to the data subject's attention at the latest at the time of the first communication with the data subject, and to be presented clearly and separately from any other information. The right to object appears in the privacy notice, in the section listing all rights, and every marketing email carries an unsubscribe link. It is not presented separately and clearly at first communication: the order confirmation email, which is the first communication with most customers, does not mention it, and in the privacy notice the right sits in a list of six rights rather than in a section of its own. Gap GAP-11 refers.

6. DATA SUBJECT RIGHTS

In the twelve months to 23 September 2026 the entity received 34 data subject requests: 11 access, 4 rectification, 14 erasure, 0 restriction, 2 portability and 3 objection. Every one was answered within the one-month period of Article 12(3). No request was refused and no fee was charged.

6.1 Procedural Requirements

OB-001, Recital 59: Modalities for exercising data subject rights

STATUS: COMPLIANT

Recital 59 requires the controller to respond to requests without undue delay and at the latest within one month, to provide means for requests to be made electronically where personal data are processed by electronic means, and to give reasons where it does not intend to comply. Requests arrive by a web form, by the privacy contact address, by post or by telephone to customer service. Each is logged the same working day in the request log, which records receipt date, right exercised, action taken and response date. The Operations Manager owns every request; the Managing Director authorises any decision not to act. The log shows a longest response time of 19 days.

OB-028, Article 12(2): Facilitating the exercise of rights

STATUS: COMPLIANT

A dedicated request form in the account area pre-fills the account identity, so a signed-in customer needs no separate identity verification. For requests from outside the account, identity is verified by matching two order details, which is proportionate and does not require identity documents. Staff training covers how to recognise a request received on any channel, including one made in a chat message or a social media reply, and how to escalate it the same day.

OB-029, Article 12(3): Response time and information

STATUS: COMPLIANT

The request log calculates the one-month deadline on entry and shows a due date on the operations dashboard. No request has required the extension of up to two further months permitted by Article 12(3). The procedure states that if an extension is needed, the data subject is told within one month of receipt, with the reasons for the delay, and the letter template for that is held with the procedure.

OB-030, Article 12(4): Reasons for refusal

STATUS: COMPLIANT

Article 12(4) requires the controller, where it takes no action, to inform the data subject without delay and at the latest within one month of the reasons and of the possibility of lodging a complaint with a supervisory authority and of seeking a judicial remedy. The refusal template carries all three elements and names the Data Protection Commission. No refusal has been issued. The log has a field for refusals, the reasons and the authorising manager, and refusal records are retained for six years.

OB-031, Article 12(5): Free of charge and manifestly unfounded or excessive requests

STATUS: COMPLIANT

All information and communications are provided free of charge. The procedure states that a reasonable fee based on administrative cost may be charged for further copies under Article 15(3), and sets that fee at the cost of media and postage. No request has been treated as manifestly unfounded or excessive. The procedure records that the burden of demonstrating that character rests on the entity and requires the Managing Director to record the evidence before any such determination.

6.2 Right of Access

OB-038, Article 15(1) to (3): Right of access

STATUS: PARTIAL

On an access request the Operations Manager searches the order platform, the marketing platform and the shared mailbox, and compiles the Article 15(1) information: purposes, categories of personal data, recipients, storage period, the rights to rectification, erasure, restriction and objection, the right to lodge a complaint, the source where the data were not collected from the data subject, and the absence of automated decision-making. The copy is provided as a PDF covering letter with a CSV extract. Third-party names appearing in customer service messages are removed before release. The gap is coverage: the customer service assistant vendor holds transcripts in its own console, and that console is not searched, so a customer who raised an enquiry through the assistant may receive an incomplete copy. Gap GAP-12 refers.

6.3 Right to Rectification

OB-039, Article 16: Right to rectification

STATUS: COMPLIANT

Article 16 requires the controller to rectify inaccurate personal data without undue delay and to complete incomplete data, including by means of a supplementary statement. Customers correct most fields themselves. Where a correction is requested for a field they cannot edit, the Operations Manager verifies the correct value against the order record or a document supplied, makes the change, and confirms it to the customer. The target is five working days and the four rectifications in the period were completed in an average of two. Where the customer disputes a value the entity cannot verify, a supplementary statement is attached to the account note and shown alongside the disputed field.

6.4 Right to Erasure

OB-040, Article 17(1): Right to erasure

STATUS: PARTIAL

The procedure tests each of the grounds in Article 17(1) in turn: data no longer necessary, consent withdrawn with no other legal ground, objection under Article 21(1) with no overriding grounds, objection under Article 21(2), unlawful processing, a legal obligation to erase, and data collected in relation to information society services offered to a child under Article 8(1). Where the ground is made out, the account and its personal data are deleted from the order platform and removed from backups at the end of the 35-day backup cycle. Where an exception in Article 17(3) applies, the entity records it: in all 14 erasure requests it retained the order and payment records needed for statutory record-keeping and told the customer which records were kept and why. The gap is propagation: erasure is not carried through to the marketing platform or to the customer service assistant vendor's console as a single action, and in two of the 14 cases the marketing record was removed only after a second request. Gap GAP-13 refers.

OB-041, Article 17(2): Erasure notification to other controllers

STATUS: NOT APPLICABLE

Ground: the entity has made no personal data public. It publishes no customer reviews carrying personal data, no customer names, and no staff directory. Article 17(2) applies only where the controller has made the personal data public, so the duty does not arise.

OB-003, Recital 66: Informing other controllers of an erasure request

STATUS: NOT APPLICABLE

Ground: Recital 66 addresses the controller who has made personal data public and requires it to inform other controllers processing those data to erase any links to, or copies or replications of, them. The entity has made no personal data public, as recorded at OB-041, so no third-party controller register and no erasure notification record are required. The review that established this was carried out on 2 February 2026 and covered the website, the product pages, the newsletter archive and the entity's social media accounts.

6.5 Right to Restriction

OB-042, Article 18(1): Right to restriction of processing

STATUS: COMPLIANT

The order platform carries a restriction flag which suspends marketing, suppresses the record from bulk exports and blocks edits while leaving the data readable for the purpose of a legal claim. The procedure covers all four grounds in Article 18(1): contested accuracy pending verification, unlawful processing where the data subject opposes erasure, data no longer needed by the controller but required by the data subject for legal claims, and an objection pending verification of the controller's legitimate grounds. Verification following an objection is completed within ten working days. Restrictions are recorded with the date imposed, the ground, and the date and reason for lifting.

OB-043, Article 18(3): Notification before lifting restriction

STATUS: COMPLIANT

Article 18(3) requires the controller to inform the data subject before lifting a restriction obtained under Article 18(1). The procedure requires written notice at least five working days before the flag is cleared, stating the reason the restriction no longer applies and what processing will resume. No restriction has been requested or lifted in the period, so the procedure is documented but untested.

6.6 Notification to Recipients

OB-044, Article 19: Notification regarding rectification, erasure or restriction

STATUS: PARTIAL

Article 19 requires the controller to communicate any rectification, erasure or restriction to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort, and to inform the data subject about those recipients if requested. The entity maintains a recipient register naming all six processors and the three separate controllers. Notification works for the processors, which are instructed through the platform or by email. It does not work for the two couriers or the payment provider: no rectification or erasure has been communicated to them, and no assessment of impossibility or disproportionate effort has been recorded to justify that. Gap GAP-14 refers. On request, the entity will tell the data subject which recipients hold their data.

6.7 Right to Data Portability

OB-045, Article 20(1): Right to data portability

STATUS: COMPLIANT

The activities carried out by automated means on consent or contract are customer accounts, order processing, payment, customer service and marketing email. The portability export is a CSV file containing account details, order history, addresses and marketing preferences, which is a structured, commonly used and machine-readable format. The classification rule is recorded: data the customer provided and data observed from their activity are included; the fraud score and the customer service quality rating, both derived by the entity, are excluded. Direct transmission to another controller has not been requested and no common interface exists in the sector, so the entity records that direct transmission is not technically feasible today and provides the file to the customer instead.

6.8 Right to Object

OB-046, Article 21(1): Right to object, legitimate interests

STATUS: COMPLIANT

The activities resting on Article 6(1)(f) are fraud screening, customer service quality review, recruitment records for unsuccessful applicants, warehouse CCTV and supplier contact management. The entity relies on no ground under Article 6(1)(e). On an objection the Operations Manager reassesses the legitimate interests assessment against the particular situation described, and the Managing Director decides. Three objections were received, all to marketing, and all were actioned under Article 21(2). No objection under Article 21(1) has been received. Where processing would continue, the procedure requires the compelling legitimate grounds to be recorded and explained to the data subject in writing.

OB-047, Article 21(2) to (3): Right to object to direct marketing

STATUS: COMPLIANT

Article 21(2) gives an unconditional right to object to processing for direct marketing. On objection the email address is added to a suppression list held in the marketing platform and retained indefinitely for the purpose of honouring the objection. The platform checks every send against the suppression list, and a re-import of an address on that list is rejected at upload. The three objections received were actioned within 24 hours. Every marketing email carries a one-click unsubscribe link and the account area carries a preference switch, which are the automated means referred to in Article 21(5).

6.9 Automated Decision-Making

OB-049, Article 22(1): Automated individual decision-making

STATUS: COMPLIANT

Article 22(1) provides that the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. The entity makes no such decision. Two candidates were examined. The fraud screening service returns a score; an order is never refused on the score alone, and the Operations Manager reviews and decides every refusal, with authority to release the order. The customer service assistant drafts replies; an agent reads, edits where needed and sends every reply, and the assistant has no authority to grant or refuse a refund, a return or a credit. The human involvement is meaningful in both cases because the reviewer has the authority and the information to reach a different outcome, and the procedure records the number of overrides: 41 of 386 flagged orders were released in the period.

OB-050, Article 22(3): Safeguards for automated decisions

STATUS: NOT APPLICABLE

Ground: Article 22(3) applies where a decision within Article 22(1) is permitted under Article 22(2)(a) or (c). No decision within Article 22(1) is made, so the safeguard duty does not arise.

7. PROCESSOR RELATIONSHIPS AND CONTRACTS

The entity engages six processors: Terrafirma Cloud GmbH (hosting, Germany), Payroll Partners (Ireland) Limited (payroll, Ireland), Orbit Support Systems B.V. (customer service assistant, Netherlands), Sendreach EU B.V. (marketing email, Netherlands), Metrix Analytics B.V. (website analytics, Netherlands) and Kilcarn Accountancy Limited (bookkeeping, Ireland). It processes personal data on behalf of no other controller.

7.1 Processor Selection

OB-007, Recital 81: Processor guarantees, contract coverage and data return or deletion

STATUS: COMPLIANT

Recital 81 requires the controller to use only processors providing sufficient guarantees in terms of expert knowledge, reliability and resources, to govern processing by a contract setting out the subject matter, duration, nature and purposes of processing, the type of personal data and the categories of data subjects, and to require the processor to return or delete personal data after the processing services end. A standard assessment questionnaire covers certifications, sub-processor lists, security measures, breach notification times and deletion procedures. It is completed before engagement and reviewed annually, with the exception recorded at OB-058. Five of the six processors hold a current independent security certification; the sixth, the accountant, is covered by a professional body's practice standard. Five of the six agreements require return or deletion at the controller's choice within 30 days of termination, and the sixth is recorded at OB-060.

OB-058, Article 28(1): Use only processors with sufficient guarantees

STATUS: PARTIAL

Article 28(1) requires the controller to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject. The processor register records, for each of the six processors, the service, the data categories reached, the date of the last assessment, the certification held and the date of the next review. The most recent assessment was the reassessment of Sendreach EU B.V. on 11 June 2026, prompted by a change to its sub-processor list; the entity requested the updated list, the region configuration and the deletion timescale, and accepted the change.

Two defects sit on one vendor. No assessment was recorded for Orbit Support Systems B.V. before the customer service assistant went live on 7 April 2026, so the entity holds no evidence that it judged the vendor's expert knowledge, reliability and resources before entrusting customer enquiries to it. The entity has also not obtained evidence that the vendor imposes equivalent data protection obligations on its own sub-processors, including the model hosting sub-processor in the United States. Gap GAP-15 refers.

7.2 Sub-processor Authorisation

OB-059, Article 28(2): Sub-processor authorisation

STATUS: NOT APPLICABLE

Ground: the duty holder under Article 28(2) is the processor. The entity acts as a controller only and engages no processor on behalf of another controller, so it holds no duty to seek authorisation for a sub-processor. As controller, the entity grants general written authorisation in each of its six agreements, with 30 days notice of any addition or replacement and a right to object. That arrangement is assessed at OB-058.

7.3 Data Processing Agreement

OB-060, Article 28(3): Mandatory contract content

STATUS: PARTIAL

Article 28(3) requires processing by a processor to be governed by a contract setting out the subject matter, the duration, the nature and purpose of the processing, the type of personal data, the categories of data subjects and the obligations and rights of the controller, and stipulating the eight processor obligations at Article 28(3)(a) to (h).

Five of the six agreements contain all five contract elements and all eight clauses. The hosting agreement, taken as the largest engagement by volume, defines the subject matter as the operation of the order platform and database, the duration as the term of the service agreement and any wind-down period, the nature and purpose as storage, hosting and backup for order fulfilment and account management, the type of personal data as identity, contact, address, order and support data, and the categories of data subjects as customers, employees and supplier contacts.

The sixth, with Orbit Support Systems B.V. for the customer service assistant, is the vendor's standard online terms. It carries clauses (a) to (f) but omits clause (g), the duty to delete or return all personal data at the choice of the controller at the end of the provision of services and to delete existing copies, and clause (h), the duty to make available all information necessary to demonstrate compliance with Article 28 and to allow for and contribute to audits, including inspections. No audit or inspection has been conducted of any processor. Gap GAP-01 refers.

Article 28(3) clause	Five agreements	Orbit Support Systems B.V.
(a) Processing only on documented instructions	Present	Present
(b) Confidentiality of authorised persons	Present	Present

Article 28(3) clause	Five agreements	Orbit Support Systems B.V.
(c) Security measures under Article 32	Present	Present
(d) Conditions for engaging sub-processors	Present	Present
(e) Assistance with data subject rights	Present	Present
(f) Assistance with Articles 32 to 36	Present	Present
(g) Deletion or return of data after service end	Present	Absent (GAP-01)
(h) Information to demonstrate compliance and audit rights	Present	Absent (GAP-01)

7.4 Sub-processor Obligations

OB-061, Article 28(4): Sub-processor contractual obligations

STATUS: NOT APPLICABLE

Ground: the duty holder under Article 28(4) is the processor. The entity acts as a controller only and appoints no sub-processor. The controller-side question of whether its processors have imposed equivalent obligations on their own sub-processors is assessed at OB-058, where the absence of that evidence for one vendor is recorded.

7.5 Written Form

OB-062, Article 28(9): Contract in writing

STATUS: COMPLIANT

Article 28(9) requires the contract referred to in Article 28(3) and (4) to be in writing, including in electronic form. All six agreements are in writing: four are signed electronically, one is a signed paper contract and one is accepted online terms. Signed copies are held in a single folder in the hosted document store, and the processor register records the counterparty, the date signed, the renewal date and the location of the signed copy. The register shows all six agreements current, none expired.

7.6 Processor Instructions

OB-063, Article 29: Processing under the authority of the controller

STATUS: COMPLIANT

Article 29 requires any person acting under the authority of the controller who has access to personal data not to process it except on instructions from the controller, unless required by Union or Member State law. All 12 staff have a confidentiality clause in their contract of employment and complete annual training covering what they may and may not do with customer data. Access is role-based: warehouse staff see delivery names and addresses only, customer service sees order and support data, and only the Managing Director and the Operations Manager reach payroll and absence records. Where a staff member believes a law requires processing outside instructions, the procedure requires the matter to be raised with the Managing Director and recorded before the processing takes place.

8. JOINT CONTROLLERS AND REPRESENTATIVES

8.1 Joint Controller Arrangement

OB-006, Recital 80: Representative for controllers not established in the Union

STATUS: NOT APPLICABLE

Ground: the entity is established in the Union, in Ireland, and processes personal data in the context of that establishment. Recital 80 addresses a controller or processor not established in the Union, so the designation duty does not arise.

OB-055, Article 26(1): Joint controller arrangement

STATUS: NOT APPLICABLE

Ground: the entity determines the purposes and means of processing alone for all thirteen recorded activities. Each data-sharing relationship was examined against joint determination. The two couriers decide for themselves how they run delivery operations and their own retention and are separate controllers for the delivery data they hold. The payment provider determines the purposes and means of card data processing and fraud analysis under its own scheme obligations and is a separate controller for that data. The six processors act only on the entity's documented instructions. No arrangement exists in which two or more parties jointly determine why and how personal data are processed.

OB-056, Article 26(2): Essence of the arrangement available to data subjects

STATUS: NOT APPLICABLE

Ground: Article 26(2) applies only where an arrangement under Article 26(1) exists. No joint controllership exists, so the publication duty does not arise.

8.2 Union Representative

OB-057, Article 27(1): Designation of a representative in the Union

STATUS: NOT APPLICABLE

Ground: Article 27(1) applies where Article 3(2) applies, that is to a controller or processor not established in the Union. The entity is established in Ireland and falls under Article 3(1), so the designation duty does not arise and no exemption under Article 27(2) needs to be claimed.

9. DATA PROTECTION BY DESIGN, DEFAULT AND SECURITY

9.1 Data Protection by Design

OB-005, Recital 78: Internal policies and measures

STATUS: PARTIAL

Recital 78 requires the controller to adopt internal policies and implement measures meeting the principles of data protection by design and by default, including minimising processing, pseudonymising personal data as soon as possible, ensuring transparency of the functions and processing of personal data, enabling the data subject to monitor the processing, and creating and improving security features. Section 6 of the Data Protection Policy, dated 12 January 2026 and owned by the Operations Manager, addresses three of the five: minimisation, transparency and security features. Pseudonymisation is applied in practice to analytics data but is not required by the policy, and the policy says nothing about enabling the data subject to monitor the processing. Gap GAP-24 refers.

OB-053, Article 25(1): Data protection by design

STATUS: PARTIAL

Article 25(1) requires the controller, at the time of determining the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards, taking into account the state of the art, the cost of implementation, the nature, scope, context and purposes of processing, and the risks. The design review is a one-page assessment completed by the Operations Manager before any new system or material change, covering what data are needed, who will see them, how long they will be kept and what could go wrong. It was completed for the returns portal in November 2025 and for the analytics change in January 2026. It was not completed for the customer service assistant before it went live on 7 April 2026. Gap GAP-16 refers. Post-launch verification is a quarterly access review against the design record, last carried out on 30 June 2026.

9.2 Data Protection by Default

OB-054, Article 25(2): Data protection by default

STATUS: COMPLIANT

Article 25(2) requires that by default only personal data which are necessary for each specific purpose are processed, applying to the amount collected, the extent of processing, the storage period and accessibility, and that personal data are not by default made accessible without the individual's intervention to an indefinite number of natural persons. Collection is limited by the nine-field checkout. The extent of processing is limited by role-based access. The storage period is limited by the retention schedule, enforced automatically for CCTV, marketing and fraud data and by scheduled job for order data. Accessibility is limited by default: a new account is private, the marketing box is unticked, the cookie banner sets no non-essential cookie until accepted, and no customer data is visible to any person outside the entity and its processors.

9.3 Security of Processing

OB-009, Recital 83: Risk evaluation and mitigation

STATUS: COMPLIANT

Recital 83 requires the controller to evaluate the risks inherent in the processing and to implement measures to mitigate them, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data. A risk register dated 12 January 2026 scores eleven risks on likelihood and impact, covering accidental destruction, loss, alteration, unauthorised disclosure and unauthorised access. Cost is recorded against each decision: hardware security keys were adopted for the four administrator accounts at EUR 220 because those accounts reach the full customer database, and were not extended to the other eight accounts, which hold no bulk export rights and use application-based multi-factor authentication instead.

OB-069, Article 32(1): Security of processing

STATUS: PARTIAL

Article 32(1) requires appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate pseudonymisation and encryption, the ongoing confidentiality, integrity, availability and resilience of processing systems and

services, the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of the measures.

Pseudonymisation: applied to website analytics, where the identifier is not joined to the account database and the IP address is truncated at collection.

Encryption: transport encryption on all customer-facing services and on all processor connections; encryption at rest on the hosted database, the document store and all backups; keys held in the hosting provider's managed key service with access limited to two administrators.

Confidentiality: role-based access, least privilege, multi-factor authentication on all 12 accounts, quarterly access review, and a documented leaver process completed within one working day.

Integrity: change control on the order platform requiring a second approver, input validation on all public forms, and audit logging of administrator actions retained for twelve months.

Availability and resilience: the hosting provider operates across two availability zones in one region, with a documented recovery time objective of four hours and a recovery point objective of 24 hours.

Restoration: daily backups held for 35 days. A full restore test was carried out on 14 May 2026 and completed in two hours and forty minutes.

Regular testing: this is the gap. The entity relies on the hosting provider's own annual penetration test and has commissioned no test, vulnerability assessment or internal audit of its own application layer, which is where the order and account data sit. No test of the entity's own measures has been completed. Gap GAP-17 refers.

OB-070, Article 32(4): Staff processing under authority

STATUS: COMPLIANT

Article 32(4) requires the controller to take steps to ensure that any natural person acting under its authority who has access to personal data does not process them except on instructions from the controller, unless required to do so by law. Instructions are documented in the Data Protection Policy and in the role-specific handling notes for warehouse, customer service and administration. Training records show date, content and a short assessment for all 12 staff, with the 2026 round completed by 6 February 2026. The escalation route for a claimed legal requirement to process outside instructions is recorded at OB-063.

9.4 Safeguards for Archiving and Research

OB-123, Article 89(1): Safeguards for archiving, research and statistics

STATUS: NOT APPLICABLE

Ground: the entity carries out no processing for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes within the meaning of Article 89(1). Sales reporting is produced from aggregate figures that are not personal data.

10. RECORDS OF PROCESSING AND SUPERVISORY COOPERATION

The entity employs 12 persons, fewer than 250. The derogation in Article 30(5) does not release it from the record-keeping obligation: its processing is not occasional, it is regular and continuous, and it includes special categories of data in the form of sickness absence records. The record is therefore maintained in full.

10.1 Controller Records

OB-008, Recital 82: Records of processing

STATUS: COMPLIANT

Recital 82 requires the controller to maintain records of processing activities under its responsibility and to cooperate with the supervisory authority and make the records available on request. The record is held as a spreadsheet in the hosted document store, owned by the Operations Manager, and was last updated on 23 September 2026 in the course of this assessment. The entity has not been asked by a supervisory authority to produce it.

OB-064, Article 30(1): Controller records of processing activities

STATUS: PARTIAL

Article 30(1) requires the record to contain the name and contact details of the controller, the purposes of the processing, a description of the categories of data subjects and of the categories of personal data, the categories of recipients, transfers to a third country or an international organisation, where possible the envisaged time limits for erasure of the different categories of data, and where possible a general description of the technical and organisational security measures referred to in Article 32(1).

Eleven of the thirteen activities carry all seven fields. Two, website analytics and recruitment, carry no envisaged erasure time limit, because none has been set. Gap GAP-18 refers. The full record as it stands at the date of assessment is reproduced below.

RECORD OF PROCESSING ACTIVITIES, ARTICLE 30(1)

Controller: Verdigris Goods Limited, Unit 7, Ardilaun Business Park, Dublin 12, Ireland. Registration number 9999999. Contact: Aoife Brennan, Operations Manager, privacy@verdigris.example. No data protection officer designated. No joint controller. No representative required.

Security measures common to every activity: transport encryption, encryption at rest, role-based access with least privilege, multi-factor authentication for all staff accounts, quarterly access review, daily backups retained 35 days, audit logging of administrator actions, annual staff training. Activity-specific measures are noted where they differ.

Ref	Purpose of processing	Categories of data subjects	Categories of personal data	Categories of recipients	Third-country transfers	Envisaged erasure time limit	Security measures
A1	Creating and maintaining customer accounts and authenticating sign-in	Customers	Name, email, password hash, telephone, delivery and billing addresses, order history, preferences	Terrafirma Cloud GmbH (processor)	None	36 months from last sign-in	Common measures; password hashing with a memory-hard function
A2	Processing and fulfilling orders, and delivering goods	Customers, gift recipients	Name, delivery address, telephone, email, order lines, delivery instructions	Terrafirma Cloud GmbH (processor), Kilcarn Accountancy Limited (processor), Corrib Logistics Limited and Rheinpost Parcel GmbH (separate controllers)	None	Six years from the end of the financial year	Common measures; delivery manifests limited to name and address
A3	Taking payment and screening transactions for fraud	Customers	Cardholder name, billing address, amount, payment token, authorisation result, fraud score	Pactum Payments Limited (separate controller)	None	Six years from the end of the financial year for transaction records; 24 months for fraud screening outcomes	Common measures; no card number is received or stored by the entity, payment fields are hosted by the provider
A4	Answering customer service enquiries, including replies drafted by the assistant, and reviewing reply quality	Customers, prospective customers	Name, email, order reference, enquiry content, transcripts, draft replies, quality rating	Orbit Support Systems B.V. (processor), Terrafirma Cloud GmbH (processor)	United States, by a sub-processor of Orbit Support Systems B.V. hosting the assistant model. Standard contractual clauses under Article 46(2)(c). No transfer impact assessment (GAP-03)	24 months from case closure	Common measures; transcripts restricted to customer service and the Operations Manager
A5	Sending marketing email to subscribers	Subscribers, customers who opted in	Name, email, consent record, open and click events	Sendreach EU B.V. (processor)	None	24 months from last engagement; suppression list retained indefinitely to honour objections	Common measures; the platform is configured to the European Union region
A6	Measuring website use	Website visitors	Pseudonymous identifier, pages viewed, device and browser type, truncated IP address	Metrix Analytics B.V. (processor)	None	Not stated (GAP-18)	Common measures; identifier not joined to the account database, IP truncated at collection

Ref	Purpose of processing	Categories of data subjects	Categories of personal data	Categories of recipients	Third-country transfers	Envisaged erasure time limit	Security measures
A7	Handling returns, refunds and warranty claims	Customers	Name, contact details, order reference, reason for return, bank details where a refund is made outside the original method	Corrib Logistics Limited and Rheinpost Parcel GmbH (separate controllers), Pactum Payments Limited (separate controller), Kilcarn Accountancy Limited (processor)	None	Six years from the end of the financial year	Common measures; bank details visible to two administrators only
A8	Keeping accounting and statutory records	Customers, suppliers, employees	Invoices, payment records, name, address, amounts	Kilcarn Accountancy Limited (processor), Revenue Commissioners (authority)	None	Six years from the end of the financial year	Common measures; ledger access limited to two administrators and the accountant
A9	Administering employment and paying staff	Employees, directors	Name, address, PPS number, bank details, salary, tax details, working time records	Payroll Partners (Ireland) Limited (processor), Revenue Commissioners (authority), pension provider	None	Six years after employment ends	Common measures; payroll data segregated from the order platform
A10	Administering sickness absence	Employees	Dates of absence, medical certificates, fitness-to-work statements	Payroll Partners (Ireland) Limited (processor)	None	Three years after the absence ends	Common measures; paper certificates in a locked cabinet, digital copies restricted to two named individuals
A11	Recruiting staff	Job applicants	CV, contact details, interview notes, right-to-work evidence	Terrafirma Cloud GmbH (processor)	None	Not stated for unsuccessful applicants (GAP-18); successful applicant records transfer to A9	Common measures; applicant folder restricted to the hiring manager and the Operations Manager
A12	Protecting stock and controlling access at the warehouse	Employees, visitors, delivery drivers	Camera images	An Garda Síochána on request	None	30 days, automatic overwrite	Common measures; four cameras covering the loading bay and stock cage only, signage at both entrances, footage retrievable by two administrators
A13	Managing supplier and business contacts	Supplier staff	Name, business email, telephone, role	Terrafirma Cloud GmbH (processor)	None	Duration of the relationship plus two years	Common measures

10.2 Processor Records

OB-065, Article 30(2): Processor records of processing activities

STATUS: NOT APPLICABLE

Ground: the entity is a controller for every activity and processes personal data on behalf of no other controller. The duty under Article 30(2) attaches to the processor and its representative, so it does not arise.

10.3 Written Form

OB-066, Article 30(3): Records in writing

STATUS: COMPLIANT

Article 30(3) requires the records under Article 30(1) and (2) to be in writing, including in electronic form. The record is an electronic spreadsheet in the hosted document store, version-controlled, included in the daily backup, restricted to the Managing Director and the Operations Manager for editing, and readable by the whole management team. It is searchable by activity reference and by recipient.

10.4 Availability to Supervisory Authority

OB-067, Article 30(4): Records available to the supervisory authority

STATUS: COMPLIANT

Article 30(4) requires the controller to make the record available to the supervisory authority on request. The procedure names the Operations Manager as responsible, sets a target of two working days from receipt of a request, and specifies delivery as a PDF export sent from the privacy contact address with the Managing Director copied. The record is reviewed quarterly and on any change to a processing activity, a processor or a retention period, so that it is current at the moment of any request. The last review was 23 September 2026.

10.5 Cooperation with Supervisory Authority

OB-068, Article 31: Cooperation with the supervisory authority

STATUS: COMPLIANT

Article 31 requires the controller and the processor and, where applicable, their representatives to cooperate, on request, with the supervisory authority in the performance of its tasks. Correspondence from the Data Protection Commission is routed to the privacy contact address, which the Operations Manager monitors daily, and is escalated to the Managing Director the same day. The one exchange with the Commission, following the breach notification of 14 March 2026, is held in a dedicated folder with every item dated. Staff training covers what to do if an authority makes contact: take the details, pass the matter to the Operations Manager the same day, and answer nothing without authority.

10.6 Compliance with Lead Authority Decisions

OB-099, Article 60(10): Compliance with lead supervisory authority decisions

STATUS: COMPLIANT

Article 60(10) requires the controller or processor, after being notified of a lead supervisory authority decision, to take the necessary measures to ensure compliance as regards all its establishments in the Union and to notify the measures taken to the lead supervisory authority. No decision has been notified to the entity. The procedure is documented: the Managing Director receives the decision, the Operations Manager prepares an action plan within ten working days, the Managing Director approves it, and the entity writes to the Data Protection Commission confirming the measures taken. Consistency across establishments is straightforward: the entity has one establishment, in Ireland, and one set of systems.

11. BREACH NOTIFICATION AND IMPACT ASSESSMENT

11.1 Breach Notification to Authority

OB-011, Recital 85: Breach notification to the supervisory authority

STATUS: COMPLIANT

Recital 85 requires the controller to notify a personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons, and to accompany a delayed notification with reasons. The Breach Response Procedure, dated 12 January 2026 and owned by the Operations Manager, has been used twice and the 72-hour deadline was met on the one occasion notification was required.

OB-071, Article 33(1): Notification to the supervisory authority within 72 hours

STATUS: PARTIAL

Detection rests on four mechanisms: alerting on failed and unusual administrator sign-ins, weekly review of the audit log, a reporting line for staff, and notification clauses in all six processor agreements. The procedure distinguishes a security incident from a personal data breach

within Article 4(12) using a three-question test on destruction, loss, alteration, unauthorised disclosure or access. Risk is assessed on a recorded scale covering the nature of the data, the number of data subjects, the ease of identification and the severity of consequence, and the Managing Director decides. The notification template carries every element of Article 33(3): the nature of the breach, the categories and approximate number of data subjects and records concerned, the contact point, the likely consequences and the measures taken or proposed. Phased notification under Article 33(4) is provided for.

Two defects remain. The procedure does not define the point at which the entity becomes aware of a breach, which is the moment the 72-hour clock starts, and it does not say who makes that determination. The escalation path is described in steps but sets no maximum time for any step, so the internal route from detection to the person authorised to notify is not bounded in hours. Gap GAP-20 refers. No tabletop exercise has been run in the last twelve months.

OB-072, Article 33(2): Processor notification to the controller

STATUS: NOT APPLICABLE

Ground: the duty under Article 33(2) attaches to the processor. The entity acts as a controller only. On the controller side, all six agreements require the processor to notify the entity without undue delay and in any event within 24 hours of becoming aware, and compliance is checked at the annual processor review.

OB-073, Article 33(5): Breach documentation

STATUS: COMPLIANT

Article 33(5) requires the controller to document any personal data breaches, comprising the facts relating to the breach, its effects and the remedial action taken, in a form that enables the supervisory authority to verify compliance. The breach register holds two entries.

Date	Facts	Effects	Remedial action	Notified
12 March 2026	A delivery manifest containing the names and addresses of 34 customers was uploaded to the wrong courier account	The receiving courier held the file for 41 hours before deletion; no evidence of further access	File deleted and deletion confirmed in writing; upload step changed to require account confirmation; the 34 customers were informed	Data Protection Commission notified 14 March 2026, 61 hours after awareness
2 July 2026	A customer service reply was sent to the wrong email address, disclosing one customer's name and order reference	One recipient, who confirmed deletion; no special category data	Recipient confirmation obtained; address-confirmation step added to the reply template; the customer was told	Not notified. Recorded assessment: unlikely to result in a risk to the rights and freedoms of a natural person, one data subject, no financial or special category data, recipient identified and deletion confirmed

The register records the facts, the effects and the remedial action for both entries. The Operations Manager maintains it.

11.2 Communication to Data Subject

OB-012, Recital 86: Communication to the data subject

STATUS: COMPLIANT

Recital 86 requires the controller to communicate a personal data breach to the data subject without undue delay where the breach is likely to result in a high risk to the rights and freedoms of natural persons, and requires the communication to describe the nature of the breach and to include recommendations to mitigate the adverse effects. The procedure separates risk, which triggers notification to the authority under Article 33, from high risk, which triggers communication to the data subject under Article 34, and applies a recorded test to the second: whether the data could be used to reach, defraud or embarrass the data subject, and whether the entity can identify and reach those affected.

OB-074, Article 34(1): Communication to the data subject

STATUS: COMPLIANT

Article 34(1) requires the controller to communicate the breach to the data subject without undue delay where it is likely to result in a high risk. The channel is direct email to the affected customers, with a postal letter where no email address is held, sent within 24 hours of the decision to communicate. The template carries the four elements of Article 34(2): the nature of the breach in clear and plain language, the contact point, the likely consequences, and the measures taken or proposed including recommendations to mitigate. Neither recorded breach reached the high-risk threshold, so no Article 34 communication has been required. The 34 customers affected in March 2026 were told as a matter of choice, with the same template, which the register records. Reliance on an exemption under Article 34(3) requires the Managing Director to record the ground before the decision is taken.

11.3 Data Protection Impact Assessment

OB-010, Recital 84: Impact assessment and prior consultation

STATUS: PARTIAL

Recital 84 requires the controller to carry out a data protection impact assessment for processing operations likely to result in a high risk to the rights and freedoms of natural persons, and to consult the supervisory authority prior to processing where the assessment indicates a high risk

that cannot be mitigated by appropriate measures. The entity had no documented method for deciding which activities require an assessment. A DPIA register was created during this assessment and now lists one entry. No assessment has produced a finding of unmitigated high risk, so no prior consultation question has arisen. Gap GAP-19 refers.

OB-075, Article 35(1): DPIA requirement

STATUS: PARTIAL

Article 35(1) requires the controller, where a type of processing using new technologies is likely to result in a high risk to the rights and freedoms of natural persons, to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data prior to the processing.

The customer service assistant was deployed on 7 April 2026 with no prior assessment. Screened against the nine criteria after the event, the processing meets two: the innovative use of a new technological solution, and the processing of data on a large scale, the assistant having handled 11,400 enquiries since deployment. An assessment was begun on 3 September 2026 and is not complete. The entity has checked its activities against the supervisory authority's published list of operations requiring an assessment and against the list of operations that do not, and no other activity is caught. Gap GAP-02 refers. This is the highest-severity finding in the report: the assessment that Article 35(1) requires before processing has been running for more than five months after processing began.

OB-076, Article 35(2): DPO consultation on the DPIA

STATUS: NOT APPLICABLE

Ground: Article 35(2) requires the controller to seek the advice of the data protection officer "where designated". No data protection officer is designated, on the ground recorded at section 12.1, so the consultation duty does not arise.

OB-077, Article 35(7): DPIA minimum content

STATUS: PARTIAL

Article 35(7) requires the assessment to contain at least a systematic description of the envisaged processing operations and the purposes of the processing, an assessment of the necessity and proportionality of the processing operations in relation to the purposes, an assessment of the risks to the rights and freedoms of data subjects, and the measures envisaged to address those risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance. The assessment in progress contains the first and the third: a description of the assistant, the data it reads and the purposes, and a risk assessment scoring seven risks. The necessity and proportionality assessment and the measures section are not written. The views of data subjects, which Article 35(9) requires the controller to seek where appropriate, have not been sought, and the entity has not recorded why that was not appropriate. Gap GAP-21 refers.

OB-078, Article 35(11): DPIA review

STATUS: PARTIAL

Article 35(11) requires the controller, where necessary, to carry out a review to assess whether the processing is performed in accordance with the assessment, at least when there is a change of the risk represented by the processing operations. No review triggers are defined, because the first assessment is not finished. Gap GAP-25 refers.

11.4 Prior Consultation

OB-079, Article 36(1): Prior consultation with the supervisory authority

STATUS: COMPLIANT

Article 36(1) requires the controller to consult the supervisory authority prior to processing where an impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. No assessment has reached that conclusion and no consultation has been made. The procedure is documented: where the residual risk after mitigation remains high, the Operations Manager prepares the submission, the Managing Director approves it, and processing does not begin, or stops, until the Commission has replied or the period in Article 36(2) has run.

OB-080, Article 36(3): Information for prior consultation

STATUS: COMPLIANT

Article 36(3) requires the controller, when consulting, to provide the respective responsibilities of the controller, joint controllers and processors, the purposes and means of the intended processing, the measures and safeguards provided to protect the rights and freedoms of data subjects, the contact details of the data protection officer, the impact assessment, and any other information requested by the supervisory authority. A submission checklist covering each item is held with the procedure. The contact details item is answered by the privacy contact point, since no data protection officer is designated. The Operations Manager assembles the submission and the Managing Director checks it for completeness before it is sent.

12. DATA PROTECTION OFFICER AND INTERNATIONAL TRANSFERS

12.1 DPO Appointment

OB-015, Recital 97: DPO appointment

STATUS: NOT APPLICABLE

Ground: no designation is required and none has been made voluntarily. Recital 97 addresses the appointment of a person with expert knowledge of data protection law and practices where the conditions in Article 37(1) are met. The assessment against those conditions is recorded at OB-081.

OB-081, Article 37(1): Mandatory DPO designation

STATUS: NOT APPLICABLE

Ground: none of the three conditions in Article 37(1) is met, and the entity has not designated a data protection officer voluntarily. The entity is not a public authority or body. Its core activity is the online sale of homeware and small electrical accessories; it does not consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, and the customer service assistant answers enquiries from customers who contact the entity rather than monitoring behaviour. Its core activities do not consist of processing special categories of data or criminal conviction data on a large scale: the only special category data are sickness absence records for up to 12 employees, which is neither a core activity nor large scale. The assessment is recorded in the Data Protection Policy and was reviewed on 12 January 2026. Data protection enquiries are handled by the Operations Manager, whose contact details are published in the privacy notice. Under this file's own rule, where the entity meets no Article 37(1) criterion and has designated no data protection officer, obligations OB-015 and OB-081 through OB-087 are recorded as NOT APPLICABLE.

OB-082, Article 37(7): Publication of DPO contact details

STATUS: NOT APPLICABLE

Ground: no data protection officer is designated, so there are no DPO contact details to publish or to communicate to the supervisory authority. The privacy notice names the Operations Manager as the contact point for data protection enquiries.

12.2 DPO Position and Tasks

OB-083, Article 38(1): Timely involvement of the DPO

STATUS: NOT APPLICABLE

Ground: no data protection officer is designated.

OB-084, Article 38(2): Resources for the DPO

STATUS: NOT APPLICABLE

Ground: no data protection officer is designated.

OB-085, Article 38(3): DPO independence

STATUS: NOT APPLICABLE

Ground: no data protection officer is designated.

OB-086, Article 38(6): DPO conflict of interests

STATUS: NOT APPLICABLE

Ground: no data protection officer is designated.

OB-087, Article 39(1): Tasks of the DPO

STATUS: NOT APPLICABLE

Ground: no data protection officer is designated. The duty under Article 39(1) attaches to the data protection officer.

12.3 International Transfers

OB-088, Article 44: General principle for transfers

STATUS: PARTIAL

Article 44 requires that any transfer of personal data to a third country or an international organisation takes place only if the conditions laid down in Chapter V are complied with, including for onward transfers. The entity makes one transfer.

Recipient	Country	Categories of data	Data subjects	Frequency	Mechanism
Model hosting sub-processor of Orbit Support Systems B.V.	United States	Customer service enquiry content, draft replies, order reference, name and email where the customer includes them	Customers and prospective customers who use the assistant	Continuous, on each enquiry	Standard contractual clauses under Article 46(2)(c), in the Orbit Support Systems B.V. terms

All other processing stays within the European Economic Area: hosting in Germany, marketing and analytics in the Netherlands, payroll and bookkeeping in Ireland. Deliveries into the United Kingdom are made through couriers established in the Union, and no personal data is transferred to any recipient in the United Kingdom. The gap is that the transfer was identified during this assessment, not before: it is absent from the Article 30 record as first supplied and has now been added, and the entity has no evidence of how onward transfers by the sub-processor are controlled. Gap GAP-22 refers. The entity relies on no adequacy decision for this transfer.

OB-089, Article 46(1): Transfers subject to appropriate safeguards

STATUS: PARTIAL

Article 46(1) requires that, in the absence of an adequacy decision under Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if it has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies are available. The safeguard relied on is the set of standard contractual clauses adopted by the Commission under Article 46(2)(c), incorporated in the vendor's terms.

No transfer impact assessment has been carried out. The entity has not assessed whether the law and practice of the destination country provide a level of protection essentially equivalent to that guaranteed within the European Economic Area, and it has therefore not considered whether supplementary measures such as encryption, pseudonymisation or additional contractual commitments are required. Gap GAP-03 refers. The clauses themselves confer enforceable rights on data subjects and a right of redress, and the vendor's terms name the Netherlands as the forum.

OB-090, Article 47(1) to (2): Binding corporate rules

STATUS: NOT APPLICABLE

Ground: the entity is not part of a group of undertakings or a group of enterprises engaged in a joint economic activity and relies on no binding corporate rules for any transfer.

OB-091, Article 49(1) second subparagraph: Transfers based on compelling legitimate interests

STATUS: NOT APPLICABLE

Ground: the entity makes no transfer that cannot be based on Article 45 or Article 46 or on a derogation in the first subparagraph of Article 49(1). Its single transfer rests on standard contractual clauses under Article 46(2)(c), so the residual route in the second subparagraph is not used and its conditions and notification duties do not arise.

OB-092, Article 49(6): Transfer documentation in the Article 30 record

STATUS: NOT APPLICABLE

Ground: Article 49(6) requires the assessment and the suitable safeguards referred to in the second subparagraph of Article 49(1) to be documented in the records referred to in Article 30. No transfer relies on that subparagraph, so the documentation duty does not arise. The transfer that does exist is recorded in the Article 30 record at activity A4 under the third-country transfer field required by Article 30(1).

12.4 Compensation Liability

OB-114, Article 82(1): Right to compensation

STATUS: COMPLIANT

Article 82(1) gives any person who has suffered material or non-material damage as a result of an infringement of the Regulation the right to receive compensation from the controller or the processor for the damage suffered. The Managing Director confirms awareness of that liability and it is recorded in the Data Protection Policy. No compensation claim has been received. Exposure is managed through a cyber and data liability insurance policy renewed on 1 April 2026, through the complaint-handling procedure, which routes any allegation of damage to the Managing Director within one working day, and through legal review of any claim before a reply is sent. The evidence the entity would rely on to show it was not in any way responsible for a damaging event, under Article 82(3), is the breach register, the audit log, the processor agreements and the processor notification records.

13. CONSOLIDATED GAP REGISTER

#	Obligation ID	Article	Gap description	Severity	Working file	Remediation action
GAP-01	OB-060	Art. 28(3)	The agreement with Orbit Support Systems B.V. omits clause (g), deletion or return of all personal data at the end of the service, and clause (h), information to demonstrate compliance and the right to audit and inspect	HIGH	File 5	Obtain a data processing addendum from the vendor carrying clauses (g) and (h) in full, or move the service to a vendor whose terms carry all eight clauses. Do not renew the current terms without them
GAP-02	OB-075	Art. 35(1)	The customer service assistant was deployed on 7 April 2026 with no data protection impact assessment. The assessment begun on 3 September 2026 is incomplete	HIGH	File 9	Complete the impact assessment. Until it is signed off, restrict the assistant to enquiries that carry no order data, or suspend its use. Record the completion date and the residual risk decision in the DPIA register
GAP-03	OB-089	Art. 46(1)	Standard contractual clauses are relied on for the transfer of customer service transcripts to the United States with no transfer impact assessment and no consideration of supplementary measures	HIGH	File 10	Carry out a transfer impact assessment for the transfer. Where the safeguards alone are insufficient, apply supplementary measures, and record both the assessment and the measures
GAP-04	OB-013	Recital 39	No time limit for erasure and no periodic review are set for website analytics data or for the records of unsuccessful job applicants	MEDIUM	File 1	Set a period and a criterion for both categories, add them to the retention schedule and the Article 30 record, and schedule the first review
GAP-05	OB-016	Art. 5(1)	The storage limitation principle is not enforced for dormant customer accounts. 7,412 accounts have had no sign-in for more than the 36 months the schedule allows	MEDIUM	File 1	Run the deletion of accounts past the 36-month point, then schedule the job monthly and evidence each run
GAP-06	OB-018	Art. 6(1)	For the four activities relying on Article 6(1)(c), the register names Irish tax and company law without citing the provision that imposes the obligation	MEDIUM	File 1	Identify and record the specific provision for each of the four activities in the lawful basis register
GAP-07	OB-024	Art. 9(1)	Sickness absence records are processed under Article 9(2)(b) without identifying the Member State law relied on and without documenting the safeguards for the fundamental rights and interests of the data subject	MEDIUM	File 1	Identify the Member State provision, record it against the activity, and write down the safeguards that apply to the health data
GAP-08	OB-019	Art. 7(1)	For 6,050 subscribers who signed up before 1 March 2024, the consent record does not hold the wording shown at the time of consent	MEDIUM	File 2	Either re-permission the pre-March 2024 segment and capture a full record, or retire that segment from marketing use
GAP-09	OB-035	Art. 14(1) to (2)	No Article 14 notice covers the personal data received from the two couriers or from the payment provider	MEDIUM	File 3	Add an indirect-collection section to the privacy notice giving the categories obtained, the sources, the purposes, the recipients and the storage periods
GAP-10	OB-036	Art. 14(3)	No timing can be evidenced for Article 14 information and no timestamped records are kept	MEDIUM	File 3	Once the notice exists, record when the information is given for each indirect source and keep the timestamps
GAP-11	OB-048	Art. 21(4)	The right to object is not presented separately and clearly at the time of first communication	MEDIUM	File 3	Add a distinct right-to-object block to the order confirmation email and give the right its own section in the privacy notice

#	Obligation ID	Article	Gap description	Severity	Working file	Remediation action
GAP-12	OB-038	Art. 15(1) to (3)	Access requests do not search the customer service assistant vendor's console, so a copy may be incomplete	MEDIUM	File 4	Add the vendor console to the search list in the request procedure and confirm the export route with the vendor
GAP-13	OB-040	Art. 17(1)	Erasure is not propagated in one action to the marketing platform and the assistant vendor. Two of fourteen cases needed a second request	MEDIUM	File 4	Make erasure a single checklist covering every system, with a sign-off line for each, and re-check the two affected records
GAP-14	OB-044	Art. 19	Rectifications, erasures and restrictions are not communicated to the two couriers or to the payment provider, and no assessment of impossibility or disproportionate effort is recorded	MEDIUM	File 4	Agree a notification route with each of the three recipients, or record the assessment that justifies not notifying them
GAP-15	OB-058	Art. 28(1)	No due diligence assessment was recorded for Orbit Support Systems B.V. before the assistant went live, and no evidence has been obtained that its sub-processor contracts carry equivalent obligations	MEDIUM	File 5	Complete the standard processor assessment for the vendor and request the sub-processor list with confirmation that equivalent obligations are imposed
GAP-16	OB-053	Art. 25(1)	The design review was not completed before the customer service assistant went live	MEDIUM	File 7	Complete the design review as part of the impact assessment at GAP-02, and make the review a release gate that cannot be skipped
GAP-17	OB-069	Art. 32(1)	No process for regularly testing, assessing and evaluating the effectiveness of the entity's own security measures. Reliance rests on the hosting provider's test	MEDIUM	File 7	Commission an application-layer test of the order platform, set a twelve-month cycle, and record the findings and the fixes
GAP-18	OB-064	Art. 30(1)	The Article 30 record carries no envisaged erasure time limit for website analytics or for recruitment	MEDIUM	File 8	Add both limits to the record once set under GAP-04
GAP-19	OB-010	Recital 84	No documented method for deciding which processing activities require an impact assessment. The DPIA register was created during this assessment	MEDIUM	File 9	Adopt the nine-criteria screening test as a written step in the design review, and record the screening outcome for every activity
GAP-20	OB-071	Art. 33(1)	The breach procedure does not define the point of becoming aware, does not name who determines it, and sets no maximum time for any escalation step	MEDIUM	File 9	Define awareness, name the decision-maker, put an hour limit on each escalation step, and run one tabletop exercise
GAP-21	OB-077	Art. 35(7)	The impact assessment in progress lacks the necessity and proportionality assessment and the measures envisaged to address the risks. The views of data subjects required by Article 35(9) have not been sought and no reason is recorded	MEDIUM	File 9	Complete both sections, and record either the views sought or the reason seeking them was not appropriate
GAP-22	OB-088	Art. 44	The transfer to the United States was not recorded before this assessment and no evidence exists of how onward transfers by the sub-processor are controlled	MEDIUM	File 10	Keep the transfer in the Article 30 record, and obtain the vendor's written confirmation of the onward transfer controls
GAP-23	OB-033	Art. 13(2)	The privacy notice does not state whether providing personal data is a contractual requirement or necessary to enter a contract, nor the consequences of not providing it	LOW	File 3	Add one paragraph to the notice covering both points for the account and checkout channels

#	Obligation ID	Article	Gap description	Severity	Working file	Remediation action
GAP-24	OB-005	Recital 78	The internal policy addresses three of the five Recital 78 principles. Pseudonymisation and enabling the data subject to monitor the processing are not addressed	LOW	File 7	Add both principles to section 6 of the Data Protection Policy at the next review
GAP-25	OB-078	Art. 35(11)	No review triggers are defined for impact assessments	LOW	File 9	Define the triggers, including any change to the assistant model, the data it reads or the volume handled, and set a review date at sign-off

14. CONSOLIDATED RECOMMENDATIONS

Priority 1 (CRITICAL gaps):

No CRITICAL gaps were identified.

Priority 2 (HIGH gaps):

1. 1. Complete the data protection impact assessment for the customer service assistant, and restrict or suspend the assistant's processing of order-related enquiries until it is signed off (GAP-02, OB-075, Article 35(1)).
2. 2. Obtain a data processing addendum from Orbit Support Systems B.V. carrying the deletion or return clause and the audit clause required by Article 28(3)(g) and (h), or move the service to a vendor whose terms carry all eight clauses (GAP-01, OB-060, Article 28(3)).
3. 3. Carry out a transfer impact assessment for the transfer of customer service transcripts to the United States and apply supplementary measures where the standard contractual clauses alone are insufficient (GAP-03, OB-089, Article 46(1)).

These three actions are one piece of work. The impact assessment at recommendation 1 is the document that identifies the contract defect at recommendation 2 and the transfer defect at recommendation 3.

Priority 3 (MEDIUM gaps):

1. 4. Run the deletion of dormant customer accounts past the 36-month point and schedule the job monthly (GAP-05, OB-016).
2. 5. Set retention periods for website analytics data and for unsuccessful applicant records, and carry them into the retention schedule and the Article 30 record (GAP-04 and GAP-18, OB-013 and OB-064).
3. 6. Cite the specific legal provision for each of the four activities resting on Article 6(1)(c) (GAP-06, OB-018).
4. 7. Identify the Member State law relied on for sickness absence records under Article 9(2)(b) and record the safeguards (GAP-07, OB-024).
5. 8. Re-permission the pre-March 2024 marketing segment or retire it (GAP-08, OB-019).
6. 9. Add an indirect-collection section to the privacy notice covering the couriers and the payment provider, and keep timestamped records of when the information is given (GAP-09 and GAP-10, OB-035 and OB-036).
7. 10. Present the right to object separately and clearly in the order confirmation email and in the privacy notice (GAP-11, OB-048).
8. 11. Add the assistant vendor's console to the systems searched on an access request (GAP-12, OB-038).
9. 12. Make erasure a single checklist covering every system, and re-check the two records that needed a second request (GAP-13, OB-040).
10. 13. Agree a notification route to the couriers and the payment provider for rectification, erasure and restriction, or record the assessment that justifies not notifying them (GAP-14, OB-044).
11. 14. Complete the processor due diligence assessment for Orbit Support Systems B.V. and obtain its sub-processor list with confirmation of equivalent obligations (GAP-15, OB-058).
12. 15. Make the design review a release gate that cannot be skipped (GAP-16, OB-053).
13. 16. Commission an application-layer security test on a twelve-month cycle (GAP-17, OB-069).
14. 17. Adopt the nine-criteria screening test as a written step in the design review and record the outcome for every activity (GAP-19, OB-010).
15. 18. Define the point of becoming aware of a breach, name the decision-maker, put hour limits on each escalation step, and run one tabletop exercise (GAP-20, OB-071).
16. 19. Complete the necessity and proportionality assessment and the measures section of the impact assessment, and record the position on seeking the views of data subjects (GAP-21, OB-077).
17. 20. Keep the United States transfer in the Article 30 record and obtain written confirmation of the onward transfer controls (GAP-22, OB-088).

Priority 4 (LOW gaps):

1. 21. Add to the privacy notice whether providing personal data is a contractual requirement and what happens if it is not provided (GAP-23, OB-033).
2. 22. Add pseudonymisation and data subject monitoring of processing to section 6 of the Data Protection Policy (GAP-24, OB-005).
3. 23. Define the review triggers for impact assessments at sign-off (GAP-25, OB-078).

15. APPENDIX: OBLIGATION COVERAGE MATRIX

Obligation ID	Article	Requirement summary	Working file	Status	Gap severity
OB-001	Recital 59	Modalities for exercising data subject rights	File 4	COMPLIANT	Not applicable
OB-002	Recital 60	Inform data subjects of processing and purposes	File 3	COMPLIANT	Not applicable
OB-003	Recital 66	Informing other controllers of an erasure request	File 4	NOT APPLICABLE	Not applicable
OB-004	Recital 74	Accountability measures	File 1	COMPLIANT	Not applicable
OB-005	Recital 78	Internal policies for design and default	File 7	PARTIAL	LOW
OB-006	Recital 80	Representative for a controller outside the Union	File 6	NOT APPLICABLE	Not applicable
OB-007	Recital 81	Processor guarantees and data return or deletion	File 5	COMPLIANT	Not applicable
OB-008	Recital 82	Records of processing activities	File 8	COMPLIANT	Not applicable
OB-009	Recital 83	Security risk evaluation	File 7	COMPLIANT	Not applicable
OB-010	Recital 84	Impact assessment and prior consultation	File 9	PARTIAL	MEDIUM
OB-011	Recital 85	Breach notification to the supervisory authority	File 9	COMPLIANT	Not applicable
OB-012	Recital 86	Communication of a breach to the data subject	File 9	COMPLIANT	Not applicable
OB-013	Recital 39	Time limits for erasure and periodic review	File 1	PARTIAL	MEDIUM
OB-014	Recital 42	Consent requirements	File 2	COMPLIANT	Not applicable
OB-015	Recital 97	DPO appointment	File 10	NOT APPLICABLE	Not applicable
OB-016	Art. 5(1)	Principles relating to processing	File 1	PARTIAL	MEDIUM
OB-017	Art. 5(2)	Accountability principle	File 1	COMPLIANT	Not applicable
OB-018	Art. 6(1)	Lawfulness of processing	File 1	PARTIAL	MEDIUM
OB-019	Art. 7(1)	Demonstrating consent	File 2	PARTIAL	MEDIUM
OB-020	Art. 7(2)	Consent request presentation	File 2	COMPLIANT	Not applicable
OB-021	Art. 7(3)	Right to withdraw consent	File 2	COMPLIANT	Not applicable
OB-022	Art. 8(1)	Child's consent for information society services	File 2	NOT APPLICABLE	Not applicable
OB-023	Art. 8(2)	Age verification	File 2	NOT APPLICABLE	Not applicable
OB-024	Art. 9(1)	Special category data prohibition	File 1	PARTIAL	MEDIUM

Obligation ID	Article	Requirement summary	Working file	Status	Gap severity
OB-025	Art. 10	Criminal conviction data	File 1	NOT APPLICABLE	Not applicable
OB-026	Art. 11(1)	Processing not requiring identification	File 1	COMPLIANT	Not applicable
OB-027	Art. 12(1)	Transparent information and communication	File 3	COMPLIANT	Not applicable
OB-028	Art. 12(2)	Facilitating data subject rights	File 4	COMPLIANT	Not applicable
OB-029	Art. 12(3)	Response time and information	File 4	COMPLIANT	Not applicable
OB-030	Art. 12(4)	Reasons for refusal	File 4	COMPLIANT	Not applicable
OB-031	Art. 12(5)	Free of charge and excessive requests	File 4	COMPLIANT	Not applicable
OB-032	Art. 13(1)	Information at collection from the data subject	File 3	COMPLIANT	Not applicable
OB-033	Art. 13(2)	Additional information at collection	File 3	PARTIAL	LOW
OB-034	Art. 13(3)	Further processing notification	File 3	COMPLIANT	Not applicable
OB-035	Art. 14(1) to (2)	Information for indirect collection	File 3	PARTIAL	MEDIUM
OB-036	Art. 14(3)	Timing of the indirect collection notice	File 3	PARTIAL	MEDIUM
OB-037	Art. 14(4)	Further processing of indirectly obtained data	File 3	COMPLIANT	Not applicable
OB-038	Art. 15(1) to (3)	Right of access	File 4	PARTIAL	MEDIUM
OB-039	Art. 16	Right to rectification	File 4	COMPLIANT	Not applicable
OB-040	Art. 17(1)	Right to erasure	File 4	PARTIAL	MEDIUM
OB-041	Art. 17(2)	Erasure notification to other controllers	File 4	NOT APPLICABLE	Not applicable
OB-042	Art. 18(1)	Right to restriction of processing	File 4	COMPLIANT	Not applicable
OB-043	Art. 18(3)	Notification before lifting a restriction	File 4	COMPLIANT	Not applicable
OB-044	Art. 19	Notification of rectification, erasure or restriction	File 4	PARTIAL	MEDIUM
OB-045	Art. 20(1)	Right to data portability	File 4	COMPLIANT	Not applicable
OB-046	Art. 21(1)	Right to object, legitimate interests	File 4	COMPLIANT	Not applicable
OB-047	Art. 21(2) to (3)	Right to object, direct marketing	File 4	COMPLIANT	Not applicable
OB-048	Art. 21(4)	Right to object notice at first communication	File 3	PARTIAL	MEDIUM
OB-049	Art. 22(1)	Automated individual decision-making	File 4	COMPLIANT	Not applicable
OB-050	Art. 22(3)	Safeguards for automated decisions	File 4	NOT APPLICABLE	Not applicable
OB-051	Art. 24(1)	Controller responsibility	File 1	COMPLIANT	Not applicable

Obligation ID	Article	Requirement summary	Working file	Status	Gap severity
OB-052	Art. 24(2)	Data protection policies	File 1	COMPLIANT	Not applicable
OB-053	Art. 25(1)	Data protection by design	File 7	PARTIAL	MEDIUM
OB-054	Art. 25(2)	Data protection by default	File 7	COMPLIANT	Not applicable
OB-055	Art. 26(1)	Joint controller arrangement	File 6	NOT APPLICABLE	Not applicable
OB-056	Art. 26(2)	Essence of the arrangement available to data subjects	File 6	NOT APPLICABLE	Not applicable
OB-057	Art. 27(1)	Designation of a representative in the Union	File 6	NOT APPLICABLE	Not applicable
OB-058	Art. 28(1)	Use only processors with sufficient guarantees	File 5	PARTIAL	MEDIUM
OB-059	Art. 28(2)	Sub-processor authorisation	File 5	NOT APPLICABLE	Not applicable
OB-060	Art. 28(3)	Mandatory contract content	File 5	PARTIAL	HIGH
OB-061	Art. 28(4)	Sub-processor contractual obligations	File 5	NOT APPLICABLE	Not applicable
OB-062	Art. 28(9)	Contract in writing	File 5	COMPLIANT	Not applicable
OB-063	Art. 29	Processing under the authority of the controller	File 5	COMPLIANT	Not applicable
OB-064	Art. 30(1)	Controller records of processing activities	File 8	PARTIAL	MEDIUM
OB-065	Art. 30(2)	Processor records of processing activities	File 8	NOT APPLICABLE	Not applicable
OB-066	Art. 30(3)	Records in writing	File 8	COMPLIANT	Not applicable
OB-067	Art. 30(4)	Records available to the supervisory authority	File 8	COMPLIANT	Not applicable
OB-068	Art. 31	Cooperation with the supervisory authority	File 8	COMPLIANT	Not applicable
OB-069	Art. 32(1)	Security of processing	File 7	PARTIAL	MEDIUM
OB-070	Art. 32(4)	Staff processing under authority	File 7	COMPLIANT	Not applicable
OB-071	Art. 33(1)	Notification to the supervisory authority within 72 hours	File 9	PARTIAL	MEDIUM
OB-072	Art. 33(2)	Processor notification to the controller	File 9	NOT APPLICABLE	Not applicable
OB-073	Art. 33(5)	Breach documentation	File 9	COMPLIANT	Not applicable
OB-074	Art. 34(1)	Communication to the data subject	File 9	COMPLIANT	Not applicable
OB-075	Art. 35(1)	DPIA requirement	File 9	PARTIAL	HIGH
OB-076	Art. 35(2)	DPO consultation on the DPIA	File 9	NOT APPLICABLE	Not applicable
OB-077	Art. 35(7)	DPIA minimum content	File 9	PARTIAL	MEDIUM
OB-078	Art. 35(11)	DPIA review	File 9	PARTIAL	LOW

Obligation ID	Article	Requirement summary	Working file	Status	Gap severity
OB-079	Art. 36(1)	Prior consultation with the supervisory authority	File 9	COMPLIANT	Not applicable
OB-080	Art. 36(3)	Information for prior consultation	File 9	COMPLIANT	Not applicable
OB-081	Art. 37(1)	Mandatory DPO designation	File 10	NOT APPLICABLE	Not applicable
OB-082	Art. 37(7)	Publication of DPO contact details	File 10	NOT APPLICABLE	Not applicable
OB-083	Art. 38(1)	Involvement of the DPO	File 10	NOT APPLICABLE	Not applicable
OB-084	Art. 38(2)	Resources for the DPO	File 10	NOT APPLICABLE	Not applicable
OB-085	Art. 38(3)	DPO independence	File 10	NOT APPLICABLE	Not applicable
OB-086	Art. 38(6)	DPO other tasks	File 10	NOT APPLICABLE	Not applicable
OB-087	Art. 39(1)	Tasks of the DPO	File 10	NOT APPLICABLE	Not applicable
OB-088	Art. 44	General principle for transfers	File 10	PARTIAL	MEDIUM
OB-089	Art. 46(1)	Transfers subject to appropriate safeguards	File 10	PARTIAL	HIGH
OB-090	Art. 47(1) to (2)	Binding corporate rules	File 10	NOT APPLICABLE	Not applicable
OB-091	Art. 49(1) second subparagraph	Derogation transfers	File 10	NOT APPLICABLE	Not applicable
OB-092	Art. 49(6)	Transfer records	File 10	NOT APPLICABLE	Not applicable
OB-099	Art. 60(10)	Compliance with lead supervisory authority decisions	File 8	COMPLIANT	Not applicable
OB-114	Art. 82(1)	Right to compensation	File 10	COMPLIANT	Not applicable
OB-123	Art. 89(1)	Safeguards for archiving, research and statistics	File 7	NOT APPLICABLE	Not applicable

Obligations listed: 95. COMPLIANT 43, PARTIAL 25, NOT APPLICABLE 27, CONCERN 0, NON-COMPLIANT 0, NOT ASSESSED 0, NOT SUBMITTED 0. Gaps: 25, comprising 0 CRITICAL, 3 HIGH, 19 MEDIUM and 3 LOW.

Report ends.