GOVERNANCE DOCS

Records of Processing Activities

Harbour Logistics

RECORD DATE	25 September 2026
BASIS	GDPR and UK GDPR Article 30, with the fields the ICO and EU supervisory authorities recommend
ROLE	Both
CONTENTS	18 processing activities; 2 processor entries
APPROVED	Operations Director, 24 Sep 2026
PREPARED BY	Governance Docs

Confidential. Prepared for Harbour Logistics. Contains a description of the organization's processing of personal data, its recipients, transfers and security measures; share on a need-to-know basis and with supervisory authorities on request.

Based on a self-assessment using information supplied by the organization. Not independently verified by Governance Docs; see "Basis of this report and limitation of liability".

CONTENTS

Where the record stands

RECORD SCORE

90 / 100

Level 2 · Developing

The main activities are listed, but gaps in the Article 30 contents or the legal basis would be questioned.

Held at Developing while 1 critical finding is open; the score alone would place it higher.

Initial · **Developing** · Defined · Managed

The score measures how complete and well supported the record is, not how much processing the organization does.

ACTIVITIES	ARTICLE 30 COMPLETE	SENSITIVE DATA	WITH TRANSFERS	FINDINGS
18	17	4	3	9

WHAT THIS RECORD TELLS YOU

- Records of processing required: With 250 or more people, Article 30 applies in full: keep a record of every processing activity, in writing, and make it available to the supervisory authority on request.
- 18 processing activities are recorded; 17 have every Article 30(1) content.
- Put right first: Transfers outside the EEA or UK with no safeguard (PA-09).
- 3 activities show two or more signs of high risk; DPIAs are done for 2.
- 3 activities send personal data outside the EEA or UK.

DO THESE FIRST

	SEVERITY	ACTION	APPLIES TO	DOCUMENT THAT CLOSES IT
1	CRITICAL	**Transfers outside the EEA or UK with no safeguard** Name the destination countries and put a transfer tool in place for each. Where you rely on standard contractual clauses, complete a transfer impact assessment.	PA-09	Procedure for International Transfers of Personal Data
2	MAJOR	**Legitimate interests with no LIA** Complete a legitimate interests assessment for each activity, or choose another lawful basis.	PA-06, PA-12 and PA-14	Legitimate Interest Assessment Form

Analysis and priorities

IN ONE SENTENCE

The record is close to complete; put a transfer safeguard in place for the offshore support centre and finish the missing LIAs and DPIA.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our records of processing cover 18 activities and meet the Article 30 contents almost in full. One gap needs a decision now: customer support data goes to an offshore provider without a legal transfer safeguard. We will put standard contractual clauses and a transfer assessment in place this month, and complete the outstanding legitimate interests and impact assessments within the quarter.

WHERE YOU STAND	You keep a full record under Article 30: 18 processing activities and 2 processor entries, with 17 activities holding every Article 30(1) content. Your record score is 90 out of 100, but the level is held at Developing because one critical finding is open: customer support data goes to an outsourced centre outside the EEA or UK with no transfer tool recorded.
WHAT IT MEANS FOR THE ORGANIZATION	The gaps sit in what backs the record rather than the record itself. 5 activities rely on legitimate interests and only 2 have an LIA done. 3 activities show two or more signs of high risk and 1 has no DPIA. One retention entry has no real limit, and one client contract lacks some Article 28 terms. A supervisory authority asking for the record would ask for these next.
WHERE TO FOCUS FIRST	Close the support centre transfer first, then complete the legitimate interests assessments and the DPIA for security logging. Tidy the supplier payments retention, finish the pharmacy client contract, and have the owner check the AI tools entry. That brings every finding within reach of this review cycle.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Put a transfer tool in place for the support centre** PA-09 Customer support and complaints	Support data leaves the EEA or UK with no safeguard, which a supervisory authority would treat as an unlawful transfer.	Sign standard contractual clauses with the outsourced support centre and start the transfer impact assessment.	Procedure for International Transfers of Personal Data	30 DAYS
2	**Complete the missing legitimate interests assessments** PA-06 Monitoring of staff IT, email and internet use · PA-12 Security logging and threat monitoring · PA-14 AI tools used by staff	Without an LIA the organization cannot show the balance favours staff monitoring, security logging and AI use.	Run the LIA for staff monitoring with the IT Manager, then repeat it for the other two activities.	Legitimate Interest Assessment Form	60 DAYS
3	**Carry out a DPIA for security logging** PA-12 Security logging and threat monitoring	Large-scale monitoring of staff and users is likely to be high risk, and Article 35 expects a DPIA before it runs.	Screen the logging scope with the managed security provider and record the DPIA outcome.	Procedure for Conducting a Data Protection Impact Assessment	60 DAYS
4	**Close the contract and retention gaps** Clients without a full Article 28 contract · Retention with no real limit	Pharmacy deliveries involve health data under a contract missing some Article 28 terms, and supplier data is kept with no time limit.	Send the pharmacy client a data processing agreement and set a retention period for supplier payment records.	Data Processing Agreement	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Sign standard contractual clauses with the support centre.
- Start the transfer impact assessment for the support centre.
- Update the processor contracts for support.

DAYS 31 TO 60

- Complete LIAs for staff monitoring, security logging and AI tools.
- Carry out the DPIA for security logging.
- Have the owner check the AI tools entry.

DAYS 61 TO 90

- Agree the data processing agreement with the pharmacy client.
- Set a retention period for supplier payments.
- Name an owner for health and safety records.

Who keeps this record, and why

CONTROLLER DETAILS, ARTICLE 30(1)(A)

Name	Harbour Logistics
Contact details	Harbour Logistics, 14 Quay Road, Portside privacy@harbourlogistics.example
Representative Article 27	Not applicable: established in the EU
Data protection officer Articles 37 to 39	Data Protection Lead, dpo@harbourlogistics.example (DPO appointed: large-scale monitoring of drivers)
Joint controllers Article 26	None recorded
Role	Both: controller for our own data, processor for clients

GENERAL DESCRIPTION OF SECURITY MEASURES, ARTICLE 30(1)(G)

Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

DOES ARTICLE 30 APPLY IN FULL?

Records of processing required

With 250 or more people, Article 30 applies in full: keep a record of every processing activity, in writing, and make it available to the supervisory authority on request.

People employed	250 people or more
Regular processing	Yes
Likely risk to people	Yes
Special category or criminal data	Yes

Article 30(3): the record is kept in writing, including in electronic form. Article 30(4): it is made available to the supervisory authority on request.

Processing activities at a glance

One line per activity, in the order they were recorded. The pages that follow give every Article 30(1) content in full.

Ref	Activity	Purposes	Data subjects	Lawful basis	Sensitive	Recipients	Transfers	Retention	Gaps
PA-01	**Recruitment and selection** People and HR	Assess applicants, arrange interviews, make and record hiring decisions, check the r…	Job applicants; referees	Contract	Art 9(2)(b)	Hiring managers; recruitment agencies; applicant tracking s…	None	Unsuccessful applicants: 6 months after the decision; …	0
PA-02	**Employee records and administration** People and HR	Manage the employment relationship: contracts, job changes, working time, leave and …	Employees; contractors; emergency contacts	Contract	None	Line managers; HR system provider; professional advisers	None	Length of employment plus 6 years	0
PA-03	**Payroll, pensions and benefits** People and HR	Pay staff, deduct and report tax and social security, run pensions and benefits.	Employees; former employees; dependants for benef…	Legal obligation	None	Tax and social security authorities; pension provider; payr…	None	6 years after the end of the tax year	0
PA-04	**Sickness absence and occupational health** People and HR	Record and manage sickness absence, pay sick pay, make adjustments and get occupatio…	Employees	Legal obligation	Art 9(2)(b)	Line managers (limited); occupational health provider; insu…	None	Length of employment plus 6 years	0
PA-05	**Driver licence and background checks** People and HR	Check driving entitlement and, for drivers delivering to pharmacies, criminal record…	Successful applicants; employees in regulated rol…	Legal obligation	Criminal	Screening provider; the official criminal records body	None	Result recorded; certificate details deleted after 6 m…	0
PA-06	**Monitoring of staff IT, email and internet use** People and HR	Protect systems and information, and investigate misuse in line with the acceptable …	Employees; contractors	Legitimate interests	None	IT and security team; managed security provider	None	Logs kept 12 months unless needed for an investigation	0
PA-07	**Vehicle telematics and driver tracking** Operations and services	Plan routes, give customers delivery times, and monitor driving safety and vehicle u…	Drivers; delivery recipients	Legitimate interests	None	Operations managers; telematics provider; clients (delivery…	None	Location history 90 days; safety events 12 months	0
PA-08	**Customer contracts and deliveries** Customers and sales	Take and fulfil orders, deliver products and services, manage the customer contract.	Customers; customer contacts at client businesses	Contract	None	Couriers; payment provider; e-commerce or ERP provider	None	Length of the contract plus 6 years	0
PA-09	**Customer support and complaints** Customers and sales	Answer questions, resolve problems and complaints, and improve service.	Customers; members of the public who contact you	Contract	None	Helpdesk or ticketing provider; ombudsman or regulator wher…	India (outsourced support centre)	3 years after the case closes	0
PA-10	**Email and SMS marketing** Marketing	Send news and offers to customers and subscribers, and keep a suppression list of pe…	Customers; newsletter subscribers	Consent	None	Email marketing platform	None	Until unsubscribe; inactive subscribers removed after …	0

PA-11	**Website analytics and cookies** Marketing	Understand how the website is used and improve it; measure campaigns.	Website visitors	Consent	None	Analytics provider; consent management provider	United States (Adequacy decision or UK adequacy regulations)	Analytics data 14 months	0
PA-12	**Security logging and threat monitoring** IT, security and premises	Detect, investigate and respond to security events.	Employees; users; website visitors	Legitimate interests	None	Managed security provider; security tool vendors	None	12 months	0
PA-13	**CCTV at the premises** IT, security and premises	Protect people, premises and property, and help investigate incidents.	Employees; visitors; members of the public	Legitimate interests	None	Security company; police on lawful request	None	30 days unless needed for an incident	0
PA-14	**AI tools used by staff** IT, security and premises	Use generative AI assistants and AI features in business software for approved tasks.	Anyone whose data staff enter into the tools: cus…	Legitimate interests	None	AI tool provider	United States (Standard contractual clauses)	30 days, as set in the admin console	0
PA-15	**Supplier payments** Finance	Pay suppliers and contractors and keep accounting records.	Sole traders and contacts at suppliers	Contract	None	Bank; accounting software provider; auditors	None	Indefinitely	0
PA-16	**Data subject requests** Legal and compliance	Handle access, erasure, objection and other rights requests within the legal time li…	Requesters; people named in the records	Legal obligation	None	Legal advisers; supervisory authority if a complaint is made	None	2 years after the request is closed	0
PA-17	**Personal data breach records** Legal and compliance	Record, assess and report personal data breaches as Article 33(5) requires.	People affected by breaches; staff involved	Legal obligation	None	Supervisory authority; affected people; insurers; forensic …	None	6 years	1
PA-18	**Health and safety and accident records** Legal and compliance	Record accidents and incidents, report them where required and meet health and safet…	Employees; visitors; contractors	Legal obligation	Art 9(2)(b)	Health and safety authority; insurers; occupational health	None	3 years from the date of the entry, longer where the l…	0

PA-01 Recruitment and selection

People and HR · Owner: HR Manager · Checked by the owner

Purposes Article 30(1)(b)	Assess applicants, arrange interviews, make and record hiring decisions, check the right to work.
Categories of data subjects Article 30(1)(c)	Job applicants; referees
Categories of personal data Article 30(1)(c)	Contact details, CV, qualifications, employment history, interview notes, test results, references, right-to-work documents; adjustments requested for interview
Categories of recipients Article 30(1)(d)	Hiring managers; recruitment agencies; applicant tracking system provider
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	Unsuccessful applicants: 6 months after the decision; successful applicants: moved to the employee file
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Contract (Article 6(1)(b))
Special category condition Article 9(2)	9(2)(b) Employment, social security and social protection law
Source	From the person directly
Processors Article 28	Applicant tracking system provider Contracts: Yes, with every processor
Systems	Applicant tracking system
Signs of high risk	Sensitive data
DPIA Article 35	Not recorded

PA-02 Employee records and administration

People and HR · Owner: HR Manager · Checked by the owner

Purposes Article 30(1)(b)	Manage the employment relationship: contracts, job changes, working time, leave and HR administration.
Categories of data subjects Article 30(1)(c)	Employees; contractors; emergency contacts
Categories of personal data Article 30(1)(c)	Identity and contact details, emergency contacts, contract and job details, working hours, leave, training and HR correspondence
Categories of recipients Article 30(1)(d)	Line managers; HR system provider; professional advisers
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	Length of employment plus 6 years
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Contract (Article 6(1)(b))
Source	From the person directly
Processors Article 28	HR system provider Contracts: Yes, with every processor
Systems	HR system; personnel files
Signs of high risk	None ticked
DPIA Article 35	Not recorded

PA-03 Payroll, pensions and benefits

People and HR · Owner: Finance Manager · Checked by the owner

Purposes Article 30(1)(b)	Pay staff, deduct and report tax and social security, run pensions and benefits.
Categories of data subjects Article 30(1)(c)	Employees; former employees; dependants for benefits
Categories of personal data Article 30(1)(c)	Salary, bank details, tax and social security numbers, pension and benefit details, deductions
Categories of recipients Article 30(1)(d)	Tax and social security authorities; pension provider; payroll provider; bank; benefits providers
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	6 years after the end of the tax year
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Legal obligation (Article 6(1)(c)) Tax and social security law
Source	From the person directly
Processors Article 28	Payroll bureau Contracts: Yes, with every processor
Systems	Payroll system
Signs of high risk	None ticked
DPIA Article 35	Not recorded

PA-04 Sickness absence and occupational health

People and HR · Owner: HR Manager · Checked by the owner

Purposes Article 30(1)(b)	Record and manage sickness absence, pay sick pay, make adjustments and get occupational health advice.
Categories of data subjects Article 30(1)(c)	Employees
Categories of personal data Article 30(1)(c)	Absence dates, fit notes, health information, occupational health reports, adjustments
Categories of recipients Article 30(1)(d)	Line managers (limited); occupational health provider; insurers
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	Length of employment plus 6 years
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Legal obligation (Article 6(1)(c))
Special category condition Article 9(2)	9(2)(b) Employment, social security and social protection law
Source	From the person directly
Processors Article 28	Occupational health provider Contracts: Yes, with every processor
Systems	HR system (restricted fields)
Signs of high risk	Sensitive data
DPIA Article 35	Not recorded

PA-05 Driver licence and background checks

People and HR · Owner: HR Manager · Checked by the owner

Purposes Article 30(1)(b)	Check driving entitlement and, for drivers delivering to pharmacies, criminal records as the role allows.
Categories of data subjects Article 30(1)(c)	Successful applicants; employees in regulated roles
Categories of personal data Article 30(1)(c)	Identity, employment and education checks, credit checks, criminal record check results
Categories of recipients Article 30(1)(d)	Screening provider; the official criminal records body
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	Result recorded; certificate details deleted after 6 months
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Legal obligation (Article 6(1)(c))
Criminal offence data authority Article 10	Permitted for delivery drivers of controlled medicines under national law, with checks limited to relevant offences
Source	From the person directly
Processors Article 28	Screening provider Contracts: Yes, with every processor
Systems	Screening provider portal
Signs of high risk	Sensitive data
DPIA Article 35	Not recorded

PA-06 Monitoring of staff IT, email and internet use

People and HR · Owner: IT Manager · Checked by the owner

Purposes Article 30(1)(b)	Protect systems and information, and investigate misuse in line with the acceptable use policy.
Categories of data subjects Article 30(1)(c)	Employees; contractors
Categories of personal data Article 30(1)(c)	System and access logs, email metadata, web browsing logs, device data
Categories of recipients Article 30(1)(d)	IT and security team; managed security provider
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	Logs kept 12 months unless needed for an investigation
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Legitimate interests (Article 6(1)(f))
Source	From the person directly
Processors Article 28	Managed security provider Contracts: Yes, with every processor
Systems	Security monitoring platform
Signs of high risk	Systematic monitoring of people; Vulnerable people, including children and employees
DPIA Article 35	DPIA done
LIA	LIA planned

FINDINGS FOR THIS ACTIVITY

MAJOR Legitimate interests with no LIA

PA-07 Vehicle telematics and driver tracking

Operations and services · Owner: Fleet Manager · Checked by the owner

Purposes Article 30(1)(b)	Plan routes, give customers delivery times, and monitor driving safety and vehicle use.
Categories of data subjects Article 30(1)(c)	Drivers; delivery recipients
Categories of personal data Article 30(1)(c)	Vehicle location, speed and driving events, driver ID, delivery times and proof-of-delivery photos
Categories of recipients Article 30(1)(d)	Operations managers; telematics provider; clients (delivery status only)
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	Location history 90 days; safety events 12 months
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Legitimate interests (Article 6(1)(f))
Source	From the person directly
Processors Article 28	Telematics provider Contracts: Yes, with every processor
Systems	Telematics platform; route planning system
Signs of high risk	Evaluation or scoring, including profiling; Systematic monitoring of people; Vulnerable people, including children and employees
DPIA Article 35	DPIA done
LIA	LIA done

PA-08 Customer contracts and deliveries

Customers and sales · Owner: Operations Manager · Checked by the owner

Purposes Article 30(1)(b)	Take and fulfil orders, deliver products and services, manage the customer contract.
Categories of data subjects Article 30(1)(c)	Customers; customer contacts at client businesses
Categories of personal data Article 30(1)(c)	Name, contact and delivery details, order and contract history, payment status
Categories of recipients Article 30(1)(d)	Couriers; payment provider; e-commerce or ERP provider
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	Length of the contract plus 6 years
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Contract (Article 6(1)(b))
Source	From the person directly
Processors Article 28	None recorded
Systems	ERP; transport management system
Signs of high risk	None ticked
DPIA Article 35	Not recorded

PA-09 Customer support and complaints

Customers and sales · Owner: Customer Service Manager · Checked by the owner

Purposes Article 30(1)(b)	Answer questions, resolve problems and complaints, and improve service.
Categories of data subjects Article 30(1)(c)	Customers; members of the public who contact you
Categories of personal data Article 30(1)(c)	Contact details, correspondence, call notes, complaint details and outcomes
Categories of recipients Article 30(1)(d)	Helpdesk or ticketing provider; ombudsman or regulator where a complaint is escalated
Transfers outside the EEA or UK Article 30(1)(e)	India (outsourced support centre) No transfer tool recorded
Time limits for erasure Article 30(1)(f)	3 years after the case closes
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Contract (Article 6(1)(b))
Source	From the person directly
Processors Article 28	Outsourced support centre; helpdesk provider Contracts: With some processors
Systems	Helpdesk platform
Signs of high risk	None ticked
DPIA Article 35	Not recorded

FINDINGS FOR THIS ACTIVITY

CRITICAL Transfers outside the EEA or UK with no safeguard

MAJOR Processors without a full Article 28 contract

PA-10 Email and SMS marketing

Marketing · Owner: Marketing Manager · Checked by the owner

Purposes Article 30(1)(b)	Send news and offers to customers and subscribers, and keep a suppression list of people who opted out.
Categories of data subjects Article 30(1)(c)	Customers; newsletter subscribers
Categories of personal data Article 30(1)(c)	Name, email or mobile number, preferences, consent records, opens and clicks
Categories of recipients Article 30(1)(d)	Email marketing platform
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	Until unsubscribe; inactive subscribers removed after 24 months
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Consent (Article 6(1)(a))
Source	From the person directly
Processors Article 28	Email marketing platform Contracts: Yes, with every processor
Systems	Email marketing platform
Signs of high risk	None ticked
DPIA Article 35	Not recorded

PA-11 Website analytics and cookies

Marketing · Owner: Marketing Manager · Checked by the owner

Purposes Article 30(1)(b)	Understand how the website is used and improve it; measure campaigns.
Categories of data subjects Article 30(1)(c)	Website visitors
Categories of personal data Article 30(1)(c)	Online identifiers, IP address, device and browser data, pages visited, cookie choices
Categories of recipients Article 30(1)(d)	Analytics provider; consent management provider
Transfers outside the EEA or UK Article 30(1)(e)	United States Adequacy decision or UK adequacy regulations
Time limits for erasure Article 30(1)(f)	Analytics data 14 months
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Consent (Article 6(1)(a))
Source	From the person directly
Processors Article 28	Analytics provider Contracts: Yes, with every processor
Systems	Website; analytics tool
Signs of high risk	Evaluation or scoring, including profiling
DPIA Article 35	Not recorded

PA-12 Security logging and threat monitoring

IT, security and premises · Owner: IT Manager · Checked by the owner

Purposes Article 30(1)(b)	Detect, investigate and respond to security events.
Categories of data subjects Article 30(1)(c)	Employees; users; website visitors
Categories of personal data Article 30(1)(c)	Security logs, IP addresses, device identifiers, alerts and investigation records
Categories of recipients Article 30(1)(d)	Managed security provider; security tool vendors
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	12 months
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Legitimate interests (Article 6(1)(f))
Source	From the person directly
Processors Article 28	Managed security provider Contracts: Yes, with every processor
Systems	SIEM; firewalls
Signs of high risk	Systematic monitoring of people; Large scale
DPIA Article 35	Likely required, none recorded
LIA	None recorded

FINDINGS FOR THIS ACTIVITY

- MAJOR Legitimate interests with no LIA
- MAJOR Likely high-risk processing with no DPIA

PA-13 CCTV at the premises

IT, security and premises · Owner: Facilities Manager · Checked by the owner

Purposes Article 30(1)(b)	Protect people, premises and property, and help investigate incidents.
Categories of data subjects Article 30(1)(c)	Employees; visitors; members of the public
Categories of personal data Article 30(1)(c)	Video images, time and location
Categories of recipients Article 30(1)(d)	Security company; police on lawful request
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	30 days unless needed for an incident
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Legitimate interests (Article 6(1)(f))
Source	From the person directly
Processors Article 28	Security company Contracts: Yes, with every processor
Systems	CCTV recorders at depots
Signs of high risk	Systematic monitoring of people
DPIA Article 35	Not recorded
LIA	LIA done

PA-14 AI tools used by staff

IT, security and premises · Owner: IT Manager · Library wording, not yet checked

Purposes Article 30(1)(b)	Use generative AI assistants and AI features in business software for approved tasks.
Categories of data subjects Article 30(1)(c)	Anyone whose data staff enter into the tools: customers, employees, contacts
Categories of personal data Article 30(1)(c)	Prompts, uploaded documents and outputs that contain personal data
Categories of recipients Article 30(1)(d)	AI tool provider
Transfers outside the EEA or UK Article 30(1)(e)	United States Standard contractual clauses
Time limits for erasure Article 30(1)(f)	30 days, as set in the admin console
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Legitimate interests (Article 6(1)(f))
Source	From the person directly
Processors Article 28	AI tool provider Contracts: Yes, with every processor
Systems	Approved AI assistant (business tier)
Signs of high risk	New technology, such as AI or biometrics
DPIA Article 35	Not recorded
LIA	None recorded

FINDINGS FOR THIS ACTIVITY

- MAJOR Legitimate interests with no LIA
- MINOR Library entries not yet checked

PA-15 Supplier payments

Finance · Owner: Finance Manager · Checked by the owner

Purposes Article 30(1)(b)	Pay suppliers and contractors and keep accounting records.
Categories of data subjects Article 30(1)(c)	Sole traders and contacts at suppliers
Categories of personal data Article 30(1)(c)	Name, contact details, bank details, invoices and payments
Categories of recipients Article 30(1)(d)	Bank; accounting software provider; auditors
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	Indefinitely **Not a time limit**
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Contract (Article 6(1)(b))
Source	From the person directly
Processors Article 28	Accounting software provider Contracts: Yes, with every processor
Systems	Accounting system
Signs of high risk	None ticked
DPIA Article 35	Not recorded

FINDINGS FOR THIS ACTIVITY

MAJOR Retention with no real limit

PA-16 Data subject requests

Legal and compliance · Owner: Data Protection Lead · Checked by the owner

Purposes Article 30(1)(b)	Handle access, erasure, objection and other rights requests within the legal time limit.
Categories of data subjects Article 30(1)(c)	Requesters; people named in the records
Categories of personal data Article 30(1)(c)	Request details, identity checks, correspondence, records disclosed
Categories of recipients Article 30(1)(d)	Legal advisers; supervisory authority if a complaint is made
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	2 years after the request is closed
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Legal obligation (Article 6(1)(c))
Source	From the person directly
Processors Article 28	None recorded
Systems	Privacy request log
Signs of high risk	None ticked
DPIA Article 35	Not recorded

PA-17 Personal data breach records

Legal and compliance · Owner: Data Protection Lead · Checked by the owner

Purposes Article 30(1)(b)	Record, assess and report personal data breaches as Article 33(5) requires.
Categories of data subjects Article 30(1)(c)	People affected by breaches; staff involved
Categories of personal data Article 30(1)(c)	Breach facts, effects, data involved, decisions and notifications
Categories of recipients Article 30(1)(d)	Supervisory authority; affected people; insurers; forensic advisers
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	6 years
Security measures Article 30(1)(g)	**Not recorded**

Lawful basis Article 6(1)	Legal obligation (Article 6(1)(c))
Source	From the person directly
Processors Article 28	None recorded
Systems	Breach register
Signs of high risk	None ticked
DPIA Article 35	Not recorded

FINDINGS FOR THIS ACTIVITY

MAJOR Activities missing contents Article 30(1) requires

PA-18 Health and safety and accident records

Legal and compliance · Checked by the owner

Purposes Article 30(1)(b)	Record accidents and incidents, report them where required and meet health and safety duties.
Categories of data subjects Article 30(1)(c)	Employees; visitors; contractors
Categories of personal data Article 30(1)(c)	Accident reports, injuries, witness details, risk assessments
Categories of recipients Article 30(1)(d)	Health and safety authority; insurers; occupational health
Transfers outside the EEA or UK Article 30(1)(e)	None outside the EEA or UK
Time limits for erasure Article 30(1)(f)	3 years from the date of the entry, longer where the law requires
Security measures Article 30(1)(g)	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.

Lawful basis Article 6(1)	Legal obligation (Article 6(1)(c))
Special category condition Article 9(2)	9(2)(b) Employment, social security and social protection law
Source	From the person directly
Processors Article 28	None recorded
Systems	Health and safety system
Signs of high risk	Sensitive data
DPIA Article 35	Not recorded

FINDINGS FOR THIS ACTIVITY

MINOR Activities with no owner

Processing carried out on behalf of controllers

Article 30(2): for each controller, its name and contact details, the categories of processing, transfers and a general description of security measures.

Ref	Controller and contact	Categories of processing	Sub-processors	Transfers	Security measures	Contract
PR-01	Retail clients (online stores), under the parcel delivery service agreement Each client's privacy contact, listed in the client register	Delivering parcels to the client's customers: names, delivery addresses, phone numbers, delivery instructions and proof of delivery	Transport management system provider; telematics provider	None	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy.	Signed, with the Article 28(3) terms
PR-02	Northfield Pharmacy Group (fictional), pharmacy@northfield.example Client DPO: dpo@northfield.example	Delivering prescriptions to patients: names, addresses, phone numbers, and the fact of a pharmacy delivery (health data)	Transport management system provider	None	Access on a need-to-know basis with single sign-on and multi-factor authentication; encryption in transit and at rest; daily backups tested quarterly; annual staff training; supplier security checks; incident response procedure; ISO 27001-aligned information security policy. Sealed packaging; recipient ID check.	In place, but missing some terms

Where the record falls short

Each finding is a gap between the record and what the GDPR asks for, with the activities it applies to and the document that closes it.

Severity	Finding	Applies to	What it means	To fix	Document that closes it
CRITICAL	**Transfers outside the EEA or UK with no safeguard**	PA-09	Chapter V allows a transfer only to a country with an adequacy decision, under an Article 46 safeguard such as standard contractual clauses, or under a narrow Article 49 derogation. Article 30(1)(e) asks the record to name the country and, for some derogations, the safeguards.	Name the destination countries and put a transfer tool in place for each. Where you rely on standard contractual clauses, complete a transfer impact assessment.	Procedure for International Transfers of Personal Data
MAJOR	**Legitimate interests with no LIA**	PA-06, PA-12 and PA-14	Relying on legitimate interests means showing that the processing passes the purpose, necessity and balancing tests. Without a legitimate interests assessment, that reasoning is not recorded.	Complete a legitimate interests assessment for each activity, or choose another lawful basis.	Legitimate Interest Assessment Form
MAJOR	**Activities missing contents Article 30(1) requires**	PA-17	Article 30(1) sets out what the record must contain for each activity. Missing across these activities: security measures. The supervisory authority can ask for the record at any time (Article 30(4)).	Complete the purposes, the categories of people and data, recipients, transfers, retention and security measures for each activity. "None" is a valid answer for recipients or transfers.	Records of Processing Activities
MAJOR	**Likely high-risk processing with no DPIA**	PA-12	These activities meet two or more of the criteria the EDPB uses to identify processing likely to be high risk. Article 35 requires a data protection impact assessment before such processing starts, or a recorded reason why it is not needed.	Carry out a DPIA for each activity, or screen it and record why one is not needed.	Procedure for Conducting a Data Protection Impact Assessment
MAJOR	**Processors without a full Article 28 contract**	PA-09	Article 28(3) requires a written contract with every processor, with the terms the article lists: acting only on instructions, confidentiality, security, sub-processors, assistance, deletion or return, and audits.	Sign a data processing agreement with each processor named, or check the provider's standard terms cover Article 28(3).	Data Processing Agreement

MAJOR	**Retention with no real limit**	PA-15	Storage limitation (Article 5(1)(e)) means keeping data no longer than the purpose needs. An entry such as "indefinitely" or "to be confirmed" is not a time limit for erasure under Article 30(1)(f).	Set a period, or the criteria that decide it, for each activity, and apply it in the systems concerned.	Retention Policy
MAJOR	**Clients without a full Article 28 contract**	PR-02	As a processor you may only act on the controller's documented instructions, set out in a contract with the Article 28(3) terms.	Agree a data processing agreement with each client.	Data Processing Agreement
MINOR	**Library entries not yet checked**	PA-14	These activities started from the library's typical wording. Until someone who knows the process has checked them, the record may describe what organizations usually do rather than what you do.	Walk through each entry with its owner, correct it, and tick it as checked.	Procedure Register of Processing Activities
MINOR	**Activities with no owner**	PA-18	Someone has to keep each entry up to date when the process, the systems or the suppliers change.	Name an owner, by role, for each activity.	Procedure Register of Processing Activities

RECORD SCORE IN DETAIL

Area	Score	Count	Weight
Controller details Contact details, representative, DPO and joint controllers are recorded (Article 30(1)(a)).	100%	4 of 4	weight 10
Article 30 contents Every activity records purposes, people, data, recipients, transfers, retention and security.	99%	125 of 126	weight 30
Lawful basis and conditions Each activity has a lawful basis, and an Article 9 or 10 condition where sensitive data is used.	100%	22 of 22	weight 15
Transfers safeguarded Every transfer outside the EEA or UK names the country and the transfer tool.	67%	2 of 3	weight 10
Retention set Each activity has a real time limit, not "indefinitely".	94%	17 of 18	weight 10
DPIAs and LIAs linked Likely high-risk activities have a DPIA, and legitimate interests has an LIA behind it.	56%	4 of 8	weight 10
Owned and checked Each activity has an owner, and library entries have been checked.	94%	33 of 35	weight 5
Processor record A processor keeps the Article 30(2) record for each client, with a contract.	75%	3 of 4	weight 5
Approved and reviewed The record has an approver, a date and a next review date.	100%	3 of 3	weight 5

Findings by severity

1 6 2

1 · Initial (0+)
A start on a record, not yet one you could hand to a supervisory authority.

2 · Developing (40+)
The main activities are listed, but gaps in the Article 30 contents or the legal basis would be questioned.

3 · Defined (60+)
A complete record for most activities, with the bases and safeguards behind it.

4 · Managed (80+)
Complete, owned, approved and linked to the assessments behind it: ready to share on request.

Keeping the record current

Maintained by	Data Protection Lead
Reviewed by the DPO or privacy lead	Yes Support centre transfers and the pharmacy contract to be closed this quarter.
Approved by	Operations Director
Approved on	24 Sep 2026
Next review by	24 Sep 2027

HOW THIS RECORD IS KEPT

Each activity has an owner who updates it when the purpose, the data, the systems, the recipients or the suppliers change. New activities are added before they start, and screened for a DPIA. The whole record is reviewed at least once a year and approved again.

Your workbook. The Excel workbook that comes with this record holds the register in the column layout regulators' templates use, with separate transfer and retention schedules and the processor record, ready to keep up to date.

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The processing activities, their contents, the checks, findings, analysis and recommendations in this record are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

Records of processing activities for Harbour Logistics, generated 25 September 2026 by Governance Docs from the organization's own entries. The findings are automated checks against GDPR Article 30 and related articles. This is not legal advice, a certification or an audit opinion.