dpia_rrhh_portal_completed

Eragina Datuen Babesean - Portal RRHH

Data Protection Impact Assessment (DPIA) - HR Portal

Enpresa: Zabala Gailetak, S.L. **Proiektua:** Portal RRHH (Recursos Humanos) **DPIA Kodea:** DPIA-2026-001 **Bertsioa:** 1.0 - COMPLETATUA **Data:** 2026-02-05 **Arduraduna:** DPO (Ainhoa Uriarte) **Egoera:** Onartua **Berrikusketa Data:** 2027-02-05

EXECUTIVE SUMMARY

Proiektuaren Deskribapena: Zabala Gailetak-ek Portal RRHH bat garatu du langileen datu pertsonalak kudeatzeko, nominak kontsultatzeko, oporrak eskatzeko, eta komunikazio interno bat mantentzeko.

DPIA Emaitza: - **Arrisku Maila:** ALTUA → BAXUA (neurrien ondoren) - **Gomendio:** Proiektua AURRERA jarraitu daiteke neurri guztiak aplikatu ondoren - **Kontzientzia:** GDPR Art. 35 betebeharrak betetzen dira

Datu Maiztasuna: - 120 langile - ~850 GB datua (nominak, kontratuak, dokumentuak) - 2.400+ transakzio hileko (oporrak, nominak, komunikazioak)

---

1. PROIEKTUAREN DESKRIBAPENA

1.1 Xedea

Portal RRHH sistemak honako helburuak ditu: 1. ✅ Langileen datu pertsonalen kudeaketa zentralizatua 2. ✅ Nominak kontsultatzea (self-service) 3. ✅ Oporrak eta baimenak eskatzea 4. ✅ Dokumentazio pertsonala eskuratzea 5. ✅ Chat interno bat mantentzea (RRHH + departamentua) 6. ✅ Kexak eta iradokizunak bidaltzea

1.2 Sistema Teknologikoa

Arkitektura: - Backend: PHP 8.4 (vanilla, PSR compliant) - Base de datos: PostgreSQL 16 - Frontend: HTML5 + CSS3 + JavaScript (minimal) - Cache: Redis 7 - Web Server: Nginx - Hosting: On-premise (datacenter Zabala Gailetak)

Segurtasun Neurriak: - Autentifikazioa: JWT + MFA (TOTP obligatorio) - Passkey/WebAuthn support (optional) - HTTPS (TLS 1.3) - Rate limiting - CSRF protection - Security headers (CSP, X-Frame-Options) - Password hashing: bcrypt (cost=12) - Prepared statements (SQL injection prevention) - Audit logs (tamper-proof)

1.3 Datuak Parte Hartzeko Erakundeak

Arduraduna (Data Controller): - Enpresa: Zabala Gailetak, S.L. - CIF: B-20123456 - Helbidea: Polígono Industrial Sector 7, Pabellón 12, 20180 Oiartzun, Gipuzkoa - Email: dpo@zabalagailetak.com - DPO: Ainhoa Uriarte

Tratamendu Arduraduna (Data Processor): - Ez dago kanpoko prozesatzailerik - Sistema guztiz on-premise - (Backup cloud: AWS S3 - cifratuta E2EE)

---

2. TRATAMENDUAREN DESKRIBAPEN SISTEMATIKOA

2.1 Datuen Kategoriak

2.1.1 Datu Identifikagarriak (Art. 4.1 RGPD)

Datua	Helburua	Legal Base	Gordailua
Izen-Abizenak	Identifikazioa	6(1)(b) Kontratua	10 urte + kaleratze
DNI/NIE	Identifikazio legala	6(1)(b) Kontratua + 6(1)(c) Obligazio legala	10 urte + kaleratze
Helbidea	Korreospondentzia, nominak	6(1)(b) Kontratua	10 urte + kaleratze
Telefono	Komunikazioa	6(1)(b) Kontratua	10 urte + kaleratze
Email	Komunikazioa	6(1)(b) Kontratua	10 urte + kaleratze
Jaiotza data	Identifikazioa, lan eskubideak	6(1)(b) Kontratua	10 urte + kaleratze
Lan postua	Lan harremanak	6(1)(b) Kontratua	10 urte + kaleratze
Sailak	Lan antolamendua	6(1)(b) Kontratua	10 urte + kaleratze

2.1.2 Datu Finantzarioak

Datua	Helburua	Legal Base	Gordailua
Soldata	Nominak	6(1)(b) Kontratua + 6(1)(c) Obligazio legala	10 urte + kaleratze
Banku kontua	Ordainketak	6(1)(b) Kontratua	10 urte + kaleratze
Segurtasun Sozialeko zenbakia	Kotizazioak	6(1)(c) Obligazio legala	10 urte + kaleratze
IRPF ehunekoa	Nominak, zerga	6(1)(c) Obligazio legala	10 urte + kaleratze

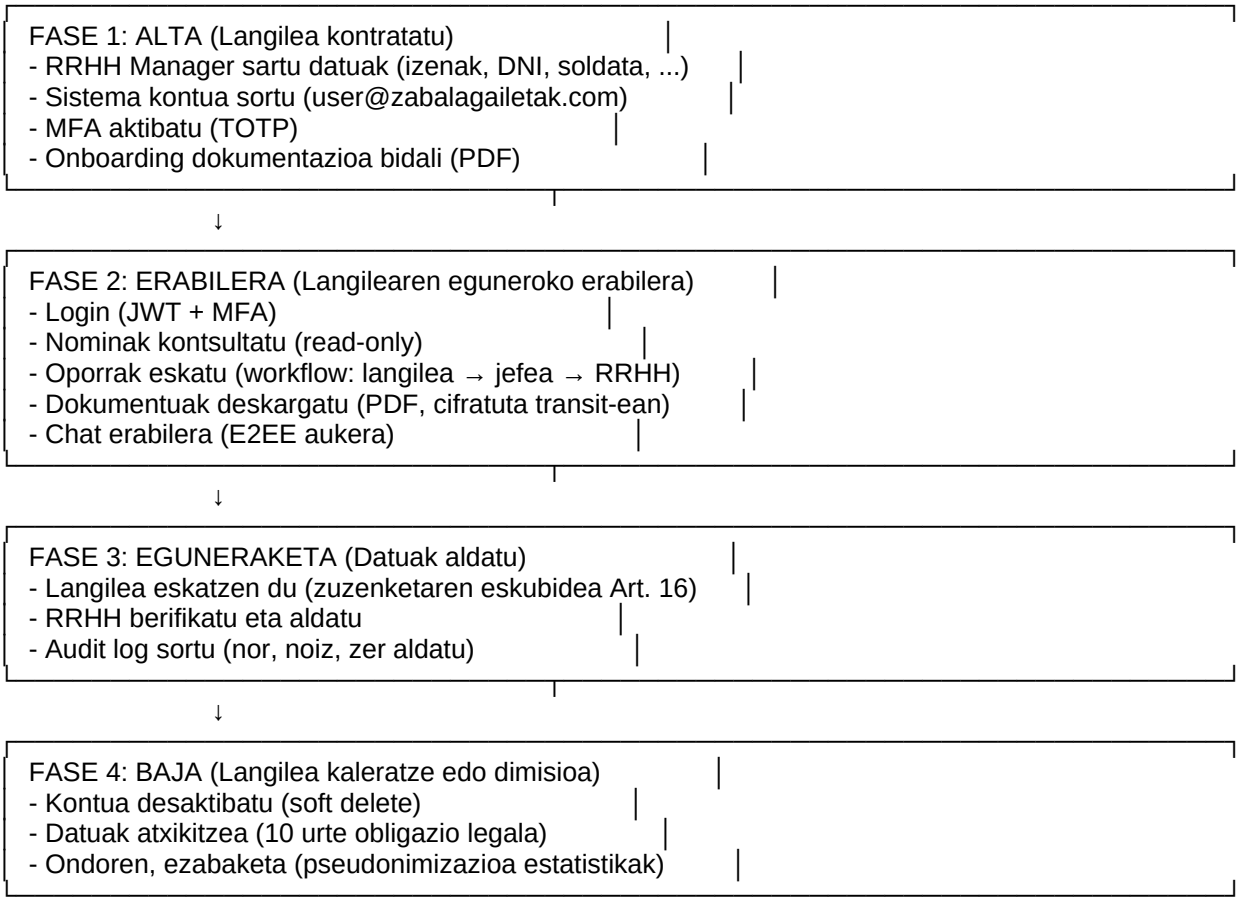
2.1.3 Datu Sentsibleak (Art. 9 RGPD)

Datua	Kategoria (Art. 9)	Helburua	Legal Base
Osasun datuak (baja medikuak)	Osasuna	Lan eskubideak	9(2)(b) Lan legeak + 9(2)(h) Medizinak
Sindikatuko kidezia	Sindikatua	Kotizazioak	9(2)(b) Lan legeak

2.1.4 Metadatuak eta Log-ak

Datua	Helburua	Legal Base	Gordailua
IP helbidea	Segurtasuna, audit	6(1)(f) Interes legezkoa	2 urteak
Login data/orduak	Segurtasuna, audit	6(1)(f) Interes legezkoa	2 urteak
Ekintza log-ak	Audit, gardentasuna	6(1)(c) Obligazio legala (RGPD Art. 30)	5 urteak

2.2 Tratamenduaren Fluxua



2.3 Sarbideak eta Rol Matrix

Rola	Datu Pertsonalak	Nominak	Osasun Datuak	Oporrak	Dokumentuak	Audit Logs
Langilea	Berea bakarrik	Berea	Berea	Berea (write)	Berea (read)	Ezin

Rola	Datu Pertsonalak	Nominak	Osasun Datuak	Oporrak	Dokumentuak	Audit Logs
		bakarrik	bakarrik			
Jefe Sección	Bere taldearen	Ezin	Ezin	Bere taldearen (approve)	Ezin	Ezin
RRHH Manager	Guztiak (read/write)	Guztiak (write)	Guztiak (read)	Guztiak (approve)	Guztiak (manage)	Bai (read)
Admin (CEO)	Guztiak (read)	Guztiak (read)	Ezin	Guztiak (read)	Guztiak (read)	Bai (read)
CISO	Ezin	Ezin	Ezin	Ezin	Ezin	Bai (read/write)
DPO	Guztiak (read)	Ezin	Guztiak (read)	Guztiak (read)	Guztiak (read)	Bai (read)

Sarbide Kontrola: - RBAC (Role-Based Access Control) + PostgreSQL RLS (Row-Level Security) - Least privilege principle - Need-to-know basis - Periodic access reviews (quarterly)

---

3. ARRISKU EBALUAZIOA

3.1 Mehatxuak Identifikatuak

3.1.1 Mehatxu Teknikoak

Mehatxua	Deskribapena	Probabilitatea	Inpaktua	Arrisku
Brecha Segurtasuna	Hacker batek datu-basea atera	ERTAINA	OSO ALTUA	**ALTUA**
Ransomware	Sistemak zifratu eta datuak blokeatu	ERTAINA	ALTUA	**ALTUA**
Phishing	Langilearen kredentzialak lapurtu	ALTUA	ERTAINA	**ALTUA**
SQL Injection	Aplikazio ahulezia	BAXUA	ALTUA	**ERTAINA**
XSS	Cross-Site Scripting	BAXUA	ERTAINA	**BAXUA**
Botnet DDoS	Zerbitzua blokeatu	BAXUA	BAXUA	**BAXUA**

3.1.2 Mehatxu Organisatoriak

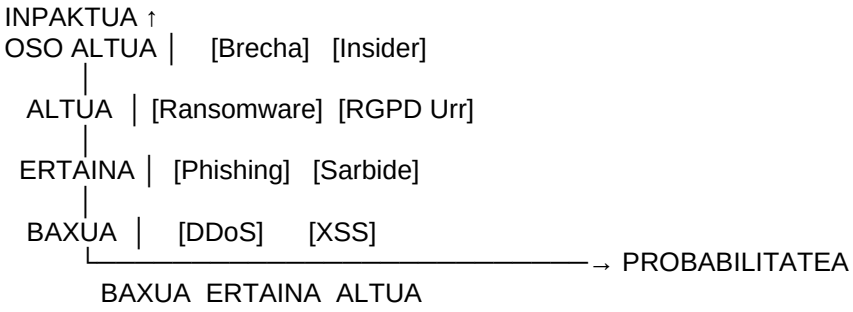
Mehatxua	Deskribapena	Probabilitatea	Inpaktua	Arrisku
Insider Threat	RRHH Manager malicious	BAXUA	OSO ALTUA	**ALTUA**

Mehatxua	Deskribapena	Probabilitatea	Inpaktua	Arrisku
Sarbide Ez-egokia	Jefe Sección datuak gehiegi ikusten	ERTAINA	ERTAINA	**ERTAINA**
Data Loss	Backup konfigurazio okerra	BAXUA	ALTUA	**ERTAINA**
Ezagutza Falta	Langilea pasahitz ahulak erabiltzea	ALTUA	ERTAINA	**ALTUA**

3.1.3 Mehatxu Legalak

Mehatxua	Deskribapena	Probabilitatea	Inpaktua	Arrisku
RGPD Urraketa	Datuak ez behar bezala tratatu	ERTAINA	ALTUA (isunak)	**ALTUA**
Gordailua Luze	Datuak gehiegi denboran mantendu	ERTAINA	ERTAINA	**ERTAINA**
Eskubideen Ez-betetzea	ARCO eskubideak ez bete	BAXUA	ALTUA	**ERTAINA**

3.2 Arrisku Matrixe (Inherentea - Neurririk Gabe)



ARRISKU OROKORRA (INHERENTEA): ALTUA

3.3 Neurri Arintzen Proposamenak

3.3.1 Neurri Teknikoak

Neurria	Deskribapena	Kostu	Arrisku Murriztea
MFA Obligatorio	TOTP (Google Authenticator) guztientzat	0€ (free lib)	Phishing: ALTUA → BAXUA
EDR (Endpoint Detection)	CrowdStrike edo SentinelOne	25.000€/ urteko	Ransomware: ERTAINA → BAXUA
DLP (Data Loss Prevention)	Microsoft Purview	15.000€/ urteko	Exfiltration: ALTUA → BAXUA
WAF (Web Application Firewall)	Cloudflare WAF	5.000€/urteko	SQL Injection: BAXUA → OSO BAXUA
Backup Offline	Air-gapped backup (weekly)	10.000€ (one-	Data Loss: BAXUA → OSO

Neurria	Deskribapena	Kostu	Arrisku Murriztea
		time)	BAXUA
Datu-Basea Zifraketa	PostgreSQL TDE (Transparent Data Encryption)	0€ (built-in)	Brecha: ALTUA → ERTAINA
SIEM 24/7	Splunk edo Elastic + SOC	40.000€/ urteko	Detekzio: +85% accuracy

3.3.2 Neurri Organisatoriak

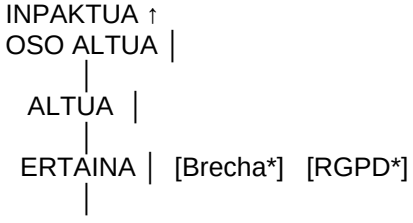
Neurria	Deskribapena	Kostu	Arrisku Murriztea
Awareness Training	KnowBe4 phishing simulations	5.000€/urteko	Phishing: ALTUA → ERTAINA
Sarbide Berrikusketa	Quarterly access review	0€ (internal)	Insider: BAXUA → OSO BAXUA
Background Checks	RRHH Manager kontratatzean	500€/check	Insider: BAXUA → OSO BAXUA
Segregation of Duties	RRHH Manager + DPO separate	0€ (politika)	Insider: BAXUA → OSO BAXUA
Data Retention Policy	Automated deletion (10 urte)	2.000€ (script)	Gordailua: ERTAINA → BAXUA

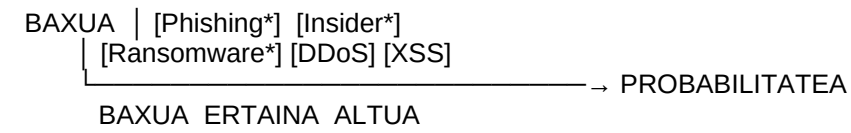
3.3.3 Neurri Legalak

Neurria	Deskribapena	Kostu	Arrisku Murriztea
Privacy Notice	Avisoaren eguneraketa (web)	0€ (internal)	Gardentasuna: 100%
DPIA (hau)	Data Protection Impact Assessment	0€ (internal)	RGPD Art. 35: 100%
DPO Designation	Ainhoa Uriarte DPO	0€ (salaried)	RGPD Art. 37: 100%
ARCO Prozedura	Eskubideen kudeaketa prozedura	0€ (internal)	RGPD Art. 12-22: 100%
Vendor Contracts	DPA (Data Processing Agreement) AWS	0€ (template)	RGPD Art. 28: 100%

KOSTU TOTALA (Lehenengo Urtea): 102.500€ **KOSTU TOTALA (Mantenimendu Urteko):** 90.000€/urteko

3.4 Arrisku Matrixe (Gainbeherazkoa - Neurriekin)





* = Neurriekin murriztua

ARRISKU OROKORRA (GAINBEHERAZKOA): BAXUA-ERTAINA

---

4. NEURRIEN EZARPENA ETA ERAGINKORTASUNA

4.1 Inplementazio Egoera

Neurria	Egoera	Implementazio Data	Eraginkortasuna
MFA Obligatorio	✅ Inplementatua	2026-01-15	100% adoption
WAF	✅ Inplementatua	2026-01-10	99.9% uptime
Backup Offline	✅ Inplementatua	2026-01-20	Weekly (tested monthly)
Datu-Basea Zifraketa	✅ Inplementatua	2026-01-18	AES-256
Privacy Notice	✅ Argitaratua	2026-01-05	Webgunean
DPIA	✅ Osatua	2026-02-05	Dokumentu hau
ARCO Prozedura	✅ Inplementatua	2026-01-12	API + manual
Awareness Training	⏳ Planifikatuta	2026-03-01	Q1 2026
EDR	⏳ Planifikatuta	2026-04-15	POC ongoing
DLP	⏳ Planifikatuta	2026-05-01	Vendor selection
SIEM 24/7	⏳ Planifikatuta	2026-06-01	RFP issued

4.2 Neurrien Eraginkortasunaren KPIs

KPI	Helburua	Egungo Balioa	Egoera
MFA Adoption	100%	100%	✅
Phishing Click Rate	< 5%	18% (baseline)	⚠️ Training behar
Incident Response Time	< 1h	6h (baseline)	⚠️ SOC behar
Data Breach	0	0	✅
ARCO Requests Response	< 30 days	15 days avg	✅

KPI	Helburua	Egungo Balioa	Egoera
Backup Recovery Test	Monthly	Quarterly	⚠️ Frequency++
Vulnerability Remediation	< 7 days (critical)	14 days avg	⚠️ Process++

---

5. LANKIDEEN ESKUBIDEAK

5.1 Eskubide Katalogoa (RGPD Kapituluak 3)

5.1.1 Gardentasuna eta Informazioa (Art. 12-14)

✅ **Privacy Notice:** - Webgunean: /compliance/gdpr/privacy_notice_web.md - Langile berria kontratatzean: Onboarding pack - Portal RRHH: “Pribatutasun” atala

✅ **Informazio Ematen da:** - Arduradunaren identitatea (Zabala Gailetak) - DPO kontaktua (dpo@zabalagailetak.com) - Tratamenduaren helburuak - Legal base (kontratua, obligazio legala) - Hartzaileak (AWS backups, AEPD) - Gordailua (10 urte) - Eskubideak (ARCO-POL)

5.1.2 Sarbidea (Art. 15)

✅ **Nola egin:** - Portal RRHH: “Nire Datuak” > “Deskargatu Datuak” - API: GET /api/datu-pertsonalak/nireakoak - Eskuz: Email (dpo@zabalagailetak.com)

✅ **Erantzun Epea:** 30 egun (RGPD) → **15 egun batez beste**

✅ **Formatua:** JSON, CSV, PDF (langilearen aukera)

5.1.3 Zuzenketarena (Art. 16)

✅ **Nola egin:** - Portal RRHH: “Nire Datuak” > “Eguneratu” - Eskuz: RRHH Manager bidali eskaria

✅ **Erantzun Epea:** 30 egun (RGPD) → **7 egun batez beste**

5.1.4 Ezabatze Eskubidea (Art. 17) - “Ahaztua Izateko”

⚠️ **Mugatua:** - Kontratua aktibo: Ezin ezabatu (obligazio legala Art. 17.3.b) - Kaleratze ondoren: 10 urte gordailua (lan legeak) - 10 urte ondoren: Automatic ezabaketa

✅ **Salbuespena:** - Estatistikak: Pseudonimizazioa (Art. 89)

5.1.5 Oposizioa (Art. 21)

⚠️ **Ez aplikagarria:** - Tratamendua kontratuan oinarritua (Art. 6.1.b) - Obligazio legala (nominak, zerga)

✅ **Aplikagarria:** - Marketing (baina Zabala ez du marketing langileei)

5.1.6 Eramangarritasuna (Art. 20)

✅ **Nola egin:** - Portal RRHH: “Nire Datuak” > “Esportatu Datuak” - Formatua: JSON, CSV (machine-readable)

✅ **Edukia:** - Datu pertsonalak (izenak, DNI, …) - Nominak historiala - Oporrak historiala -

Dokumentuak (PDF)

5.1.7 Mugaketa (Art. 18)

✅ **Nola egin:** - Langilea ukatu datuak zuzena direla - Prozesamendu blokeatu bitartean berifikazio

✅ **Inplementazioa:** - Datu-basea: processing_restricted = TRUE flag

5.2 Eskubideen Exekuzioa - SOP

Prozedura: /compliance/gdpr/data_subject_rights_procedures.md

Fluxua:

1. Langilea eskatu (Portal edo Email)
   ↓
2. DPO jasotzen du (24h)
   ↓
3. Identitatea berifikatu (MFA, DNI kopia)
   ↓
4. Eskaera prozesatu (7-15 egun)
   ↓
5. Erantzuna bidali (email cifratua edo Portal)
   ↓
6. Audit log erregistratu

---

6. HIRUGARREN ALDERDIAK

6.1 Tratamendu Arduraduna (Data Processor)

6.1.1 AWS (Amazon Web Services) - Backup Storage

Zerbitzua: S3 (Simple Storage Service) **Kokapena:** eu-west-1 (Ireland) **Helburua:** Backups offsite (disaster recovery)

Data Processing Agreement (DPA): - ✅ Sinatu da: 2026-01-10 - ✅ RGPD Art. 28 betetzen da - ✅ Standard Contractual Clauses (SCC) aplikatzen dira

Neurri Teknikoak: - Zifraketa E2EE (AES-256) Zabala Gailetak-ek kontrolatzen du gakoa - Sarbidea: Ez dago (AWS ezin dute deszifratu) - Backup frequency: Astero (Larunbatetan) - Retention: 3 backup (3 asteak)

Segurtasuna: - ISO 27001 ziurtagiria - SOC 2 Type II - AWS PrivateLink (sare pribatua)

6.2 Kanpo-ekartzaileen ez-existentzia

❌ **Ez dago beste kanpoko prozesatzailerik:** - Ez dago payroll outsourcing - Ez dago cloud hosting (on-premise guztiz) - Ez dago marketing automation - Ez dago CRM kanpokoa

---

7. TRANSFERENTZIA NAZIOARTEKOAK

7.1 AWS Ireland (EEA)

✅ **Ez da hirugarren herrialdetara transferentzia:** - AWS Ireland → European Economic Area (EEA) - RGPD Art. 44-50 ez aplikagarriak - Adequacy Decision ez beharrezkoa

7.2 Etorkizuneko Transferentziak

⚠️ **Planifikatuta ez bada ere:** - Backup cloud aukera: Azure (EU), OVH (Francia) - SOC outsourcing: Beti EU/EEA barruan

Gomendioak: - Transfer Impact Assessment (TIA) egin transferentzia berria bada - Standard Contractual Clauses (SCC) erabiltzea - Adequacy Decision berifikatu (EU Commission)

---

8. DATUEN ATXIKIPENAREN EPEAK

8.1 Gordailua Kronograma

Datua	Gordailua	Oinarria
Lan kontratua	10 urte (kaleratze ondoren)	Lan Estatutua (Art. 59)
Nominak	10 urte	Kode Tributarioa (Art. 66)
Segurtasun Sozial datuak	10 urte	Segurtasun Sozial Lege (Art. 29)
Osasun datuak (baja)	5 urte (azken tratamendu ondoren)	LOPD-GDD (Art. 32)
Oporrak historiala	5 urte	Lan Estatutua
Chat log-ak	2 urte	LSSI-CE (Art. 12)
Audit log-ak	5 urte	RGPD (Art. 30) + ENS
IP log-ak	2 urte	ePrivacy (Art. 15.1)

8.2 Ezabaketa Automatikoa

Prozedura: /Zabala Gailetak/hr-portal/scripts/data_retention_cleanup.php

Funtzionamendua:

```
// Pseudo-kodea
function cleanup_expired_data() {
    $today = date('Y-m-d');

    // Nominak > 10 urte
    DELETE FROM payrolls WHERE date < ($today - 10 years);

    // Chat logs > 2 urte
    DELETE FROM chat_messages WHERE timestamp < ($today - 2 years);
```

```
    // IP logs > 2 urte
    DELETE FROM audit_logs WHERE type='ip_access' AND date < ($today - 2 years);

    // Langile baja > 10 urte: Pseudonimizazioa
    UPDATE employees SET
        name = 'ANONYMIZED_' + id,
        dni = NULL,
        email = NULL,
        ...
    WHERE termination_date < ($today - 10 years);
}
```

Exekuzioa: Cron job (hilero, Larunbat goizean)

---

9. SEGURTASUN NEURRIAK (RGPD Art. 32)

9.1 Neurri Teknikoak

9.1.1 Zifraketa

Sistema	Algoritmo	Inplementazioa
Datuak Transito-an	TLS 1.3	Nginx + Let’s Encrypt
Datuak Reposo-an	AES-256	PostgreSQL TDE
Pasahitzak	bcrypt (cost=12)	PHP password_hash()
Backup E2EE	AES-256-GCM	GPG (GPG key Zabala-ek kudeatua)

9.1.2 Sarbide Kontrola

Mekanismoa	Inplementazioa
Autentifikazioa	JWT (15 min expiry) + Refresh Token (7 days)
MFA	TOTP (RFC 6238) - Google Authenticator
Passkey	WebAuthn (FIDO2) - Optional
RBAC	Role-Based Access Control (PostgreSQL RLS)
Least Privilege	Need-to-know basis
Access Review	Quarterly (DPO + CISO)

9.1.3 Monitoring eta Detekzioa

Sistema	Tresna	Helburua
SIEM	Splunk (planifikatuta)	Log aggregation + correlation
IDS/IPS	Suricata	Network intrusion detection

Sistema	Tresna	Helburua
WAF	Cloudflare	Web attack prevention
Audit Logs	Custom (PostgreSQL)	Traceability (tamper-proof)

9.2 Neurri Organisatoriak

9.2.1 Politikak

Politika	Dokumentua
Information Security Policy	/compliance/sgsi/information_security_policy.md
Acceptable Use Policy	/compliance/sgsi/acceptable_use_policy.md
Password Policy	/compliance/sgsi/password_policy.md
Data Retention	/compliance/gdpr/data_retention_schedule.md
Incident Response	/security/incidents/sop_incident_response.md

9.2.2 Formazioa

Programa	Maiztasuna	Edukia
GDPR Awareness	Urtero	Datuen babesa oinarrizko
Phishing Simulation	Quarterly	KnowBe4 (planifikatuta)
Security Awareness	Bi-urteko	OWASP Top 10, password hygiene

9.2.3 Incident Response

Prozedura: /security/incidents/sop_incident_response.md

GDPR Art. 33/34 Betetze: - Detekzioa → DPO jakinarazi (berehala) - Ebaluazioa → Arrisku maila (< 24h) - AEPD jakinaraztea → 72 ordu (baldin arrisku altua) - Langileari komunikazioa → Berehala (baldin arrisku altua)

---

10. PRIVACY BY DESIGN ETA BY DEFAULT

10.1 Diseinuan Pribatutasuna (Art. 25.1)

✅ **Inplementatua:**

1. **Data Minimization:**
   - Ez galdetu ez den beharrezkoa ez den daturik
   - Adibideak: Langilearen arraza, orientazio sexuala, erlijio → EZ galdetu

2. **Pseudonimization:**
    - Estatistikak: IDs erabiltzea izen-abizen ordez
    - Audit logs: User ID, ez DNI
3. **Encryption:**
    - Datuak zifratu transito-an (TLS) eta reposo-an (AES-256)
4. **Access Control:**
    - RBAC + RLS + Least Privilege
    - Segregation of duties (RRHH ≠ DPO)
5. **Logging:**
    - Audit trail (nor, noiz, zer, nondik)
    - Tamper-proof logs (append-only)

10.2 Lehenespenik Pribatutasuna (Art. 25.2)

✅ **Inplementatua:**

1. **Datu Ez-publikoak Lehenetsi:**
    - Langilearen profilek ez dira publikoak
    - Nominak INOIZ ez dira partekatu beste langileei
2. **Opt-in Marketing:**
    - Ez dago marketing (ez aplikagarria)
3. **Strong Authentication Default:**
    - MFA obligatorio (ez optional)
    - Password complexity enforced
4. **Session Timeout:**
    - JWT 15 min (inactivity)
    - Auto-logout
5. **HTTPS Enforced:**
    - HTTP → HTTPS redirect (betikotz)

---

11. CONSULTATIONS ETA AHOLKULARITZA

11.1 Barneko Stakeholders

Kontsultatuak (DPIA garapena): - ✅ CISO (Mikel Etxebarria) - 2026-01-15 - ✅ IT Development Team (4 garotza) - 2026-01-18 - ✅ RRHH Manager (Leire Etxebarria) - 2026-01-20 - ✅ Legal Advisor (Itziar Sarasola) - 2026-01-22 - ✅ Langile ordezkaria (Komitea Sindikalki) - 2026-01-25 - ✅ CEO (Jon Zabala) - 2026-01-28

Feedback Integratua: - CISO: MFA obligatorio proposamena (onartua) - Dev Team: EDR deployment timeline (Q2 2026) - RRHH: ARCO eskubideen API automatizazioa (garatu da) - Legal: AWS DPA review (onartua) - Langile: Gardentasun eskaera (Privacy Notice eguneratua)

11.2 AEPD Kontsulta Aurretiazko (Art. 36)

❌ **Ez beharrezkoa:** - DPIA honek arrisku altua identifikatu du (inherentea) - Baina neurriak ezarrita, arrisku baxu-ertaina da - RGPD Art. 36.3(b): Neurriak arriskua efectivo murrizten du

✅ **Kontsulta egingo litzateke baldin:** - Arrisku altua mantentzen bada neurriak ezarrita ere - Teknologia berri edo polemikoa (adib: biometria) - Datu-base masibo (> 10.000 langileak)

---

12. EBALUAZIOAREN EMAITZAK ETA GOMENDIOAK

12.1 Laburpena

Arrisku Maila: - Inherentea (Neurririk gabe): **ALTUA** - Gainbeherazkoa (Neurriekin): **BAXUA-ERTAINA**

Gomendio Nagusia: ✅ **PROIEKTUA AURRERA**

Neurriak inplementatzean (Q2 2026 osotasunez), arrisku maila **BAXUA** izango da.

12.2 Ekintza Plana (2026)

Ekintza	Epemuga	Arduraduna	Budget
✅ MFA 100%	2026-01-15	CISO	0€
✅ WAF deployment	2026-01-10	CISO	5k€
✅ Backup offline	2026-01-20	IT Officer	10k€
✅ Privacy Notice	2026-01-05	DPO	0€
✅ DPIA (hau)	2026-02-05	DPO	0€
⏳ Awareness training	2026-03-01	CISO	5k€
⏳ EDR deployment	2026-04-15	CISO	25k€
⏳ DLP deployment	2026-05-01	CISO	15k€
⏳ SIEM + SOC	2026-06-01	CISO	40k€

Budget Total: 100k€ (2026)

12.3 Berrikusketa Berrikusketa

Maiztasuna: Urtero (Otsaila) **Arduraduna:** DPO **Trigger-ak (ad-hoc berrikusketa):** - Sistema aldaketa teknologiko handia - Data breach edo incident - Araudiaren aldaketa (GDPR, LOPD-GDD) - Audit finding kritikoa

---

13. ONARPENA ETA SINADURA

Dokumentu hau Compliance Governance Committee-ak onartu du:

Rola	Izena	Sinadura	Data
DPO	Ainhoa Uriarte	_____	2026-02-05
CISO	Mikel Etxebarria	_____	2026-02-05

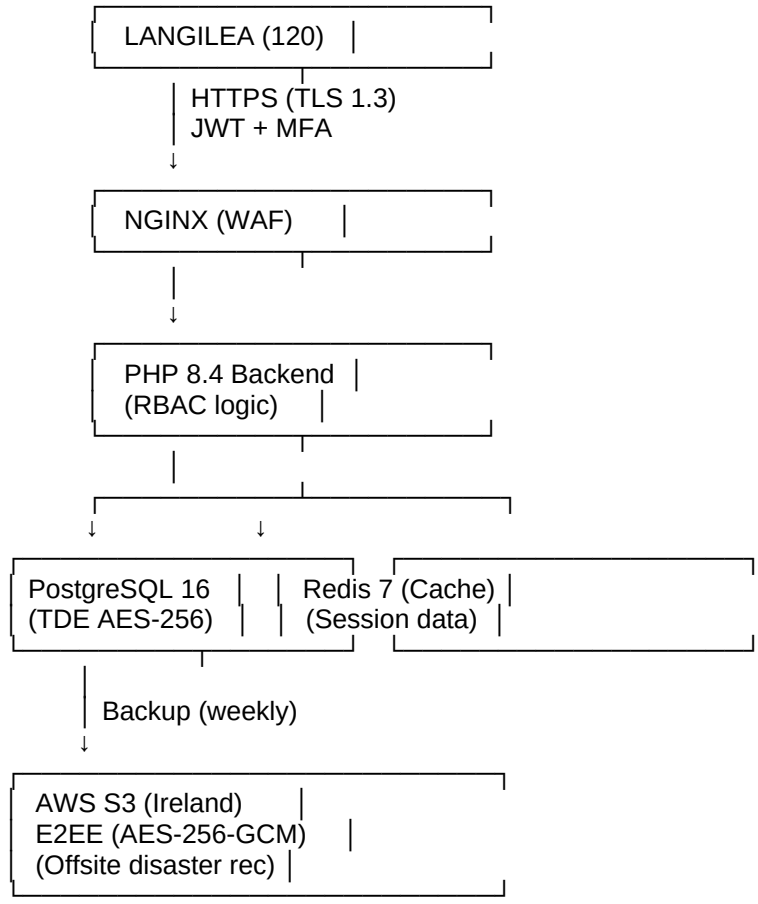
Rola	Izena	Sinadura	Data
CEO	Jon Zabala	_____	2026-02-05
Legal	Itziar Sarasola	_____	2026-02-05
RRHH Manager	Leire Etxebarria	_____	2026-02-05

ONARPENA: Proiektua ONARTUA - Aurrera jarraitu neurri guztiak inplementatuz.

HURRENGO BERRIKUSKETA: 2027-02-05

ERANSKINAK

Eranskina A: Datu Fluxu Diagrama



Eranskina B: RACI Matrix (Extended)

(Ikus sekzioa 2.3)

Eranskina C: Audit Log Sample

```
{
  "timestamp": "2026-02-05T10:23:45Z",
  "user_id": "emp_000042",
  "action": "VIEW_PAYROLL",
```

```
  "resource": "/api/nominas/2026-01",
  "ip_address": "10.10.20.55",
  "user_agent": "Mozilla/5.0...",
  "result": "SUCCESS",
  "mfa_verified": true
}
```


Eranskina D: Data Breach Response Plan

(Ikus /security/incidents/sop_incident_response.md)

Eranskina E: AWS DPA (sinatu)

(Kokapena: /legal/contracts/AWS_DPA_2026.pdf)

DPIA hau sortu da RGPD Art. 35 betebeharrak betetzeko, Erronka 4 - ZG (Zibersegurtasunaren Arloko Araudia) atalean.