GDPR Urraketa Erantzun Prozedura (Hobetua)

GDPR Data Breach Response SOP (Improved)

Enpresa: Zabala Gailetak, S.L. **Dokumentu Kodea:** GDPR-SOP-001 **Bertsioa:** 2.0 - IMPROVED POST-APT **Data:** 2026-02-05 **Jabea:** DPO **Egoera:** Indarrean

---

1. RGPD ART. 33/34 BETEBEHARRAK

1.1 Art. 33 - Jakinarazpena Autoritate Eskudunari (AEPD)

Epemuga: 72 ordu urraketa detektatu ondoren **Nori:** AEPD (Agencia Española de Protección de Datos) **Nola:** https://www.aepd.es/notificaciones-brechas

1.2 Art. 34 - Komunikazioa Interesdunari

Epemuga: BEREHALA (sin dilación indebida) **Nori:** Langileari, bezeroari (afektatuak) **Noiz OBLIGATORIO:** Arrisku ALTUA pribatutasun eskubideetarako

---

2. BREACH RESPONSE FLUXUA (72H)

```
T+0h: DETEKZIOA
  ↓
T+1h: BERIFIKAZIO ETA EBALUAZIO INICIAL
  ↓
T+4h: CONTAINMENT (isolamendua)
  ↓
T+12h: IMPACT ASSESSMENT (arrisku maila)
  ↓
T+24h: JAKINARAZPENA AEPD (baldin arrisku > ertaina)
  ↓
T+24h: KOMUNIKAZIOA AFEKTATUEI (baldin arrisku altua)
  ↓
T+72h: TXOSTEN OSOA AEPD
```

---

3. BREACH SEVERITY MATRIX

Criteria	Baxua	Ertaina	Altua	Oso Altua
Datu Kopurua	< 10	10-100	100-1000	> 1000
Datu Mota	Ez-sentsibl	Pertsonala	Finantza	Osasuna
Exfiltration	Ez	Suspekta	Konfirmatua	Publikatua
Zifraketa	Bai	Bai	Ez	Ez

Jakinarazpena AEPD: ERTAINA, ALTUA, OSO ALTUA **Komunikazioa Afektatuei:** ALTUA, OSO ALTUA

---

4. BREACH NOTIFICATION TEMPLATE (AEPD)

Web Form: https://www.aepd.es/notificaciones-brechas

Edukia (Art. 33.3):

1. **Urraketa Deskribapena:**
    - Data eta ordua
    - Nola gertatu da (ransomware, phishing, insider, …)
    - Non gertatu da (sistemak afektatuak)
2. **Datu Kategoriak eta Kopurua:**
    - Kategoria: Izen-abizenak, DNI, emailak, nominak, osasun datuak, …
    - Kopurua: 120 langile afektatuak
3. **DPO Kontaktua:**
    - Izena: Ainhoa Uriarte
    - Email: dpo@zabalagailetak.com
    - Telefono: +34 943 XX XX XX
4. **Ondorio Posibleak:**
    - Arrisku: Identitate lapurreta, fraude finantzaria, diskriminazio
    - Probabilitate: Altua / Ertaina / Baxua
5. **Neurri Adoptatzea:**
    - Containment: Sistemak isolatu
    - Eradication: Malware ezabatu

- Recovery: Backup berr eskuratzea
- Notification: Afektatuei jakinarazi

6. **Neurri Arintzen Hartuak:**
   - MFA aktibatu (100%)
   - EDR deployment
   - Password reset (guztiak)
   - Credit monitoring offer (afektatuei)

---

5. BREACH NOTIFICATION TEMPLATE (AFEKTATUEI)

Bidalketa: Email (cifratua) + Posta fisikoa

Template:

```
Asunto: INFORMAZIO GARRANTZITSUA - Datu Pertsonalen Urraketa

Estimado/a [IZENA]:

Zabala Gailetak, S.L.-k zibersegurtasun intzidentzia bat jasan du [DATA],
eta zure datu pertsonalak konprometitu egin dira.

DATUAK AFEKTATUAK:
- Izen-abizenak
- DNI
- Helbidea
- Telefono
- Email
- [Baldin finantza] Banku kontuaren zenbakia
- [Baldin osasun] Osasun datuak (baja medikuak)

ZER GERTATU DA:
[Deskribapen laburra: Adib: Ransomware erasoa datuak exfiltratu zituen]

ARRISKU POSIBLEAK:
- Identitate lapurreta
- Fraude finantzaria (baldin banku datuak)
- Phishing erasoak zure izenean

NEURRI HARTUAK ZABALA GAILETAK-EK:
- Sistemak isolatu eta aseguratu
- Pasahitz guztiak aldatu
- MFA aktibatu (100%)
- EDR segurtasun sistema instalatu
- AEPD jakinarazi (72h barruan)

NEURRI HARTU BEHAR DITUZU ZUK:
```

```
1. Pasahitzak aldatu (batez ere banku, email)
2. Aktibatu MFA zure kontu guztietan
3. Monitorizatu banku mugimendua (fraud alert)
4. Phishing email-en kontuz ibili

LAGUNTZA:
- Credit monitoring zerbitzua: DOAKO 2 urtean
- DPO kontaktu: dpo@zabalagailetak.com
- Telefono laguntza: +34 943 XX XX XX (09:00-18:00)

ZURE ESKUBIDEAK:
- Erreklamazioa AEPD-ra: https://www.aepd.es
- Kalte-ordaina eskatzea (RGPD Art. 82)

Sentitzen dugu egoera hau. Gure lehentasuna zure datuak babestea da.

Eskerrik asko zure ulertzeagatik.

Jon Zabala
CEO, Zabala Gailetak, S.L.
```

---

6. BREACH RESPONSE TEAM

Rol	Izena	Telefono	Ardurak
Incident Commander	CISO (Mikel Etxebarria)	+34 XXX	Koordinazio orokorra
DPO	Ainhoa Uriarte	+34 XXX	AEPD jakinarazpena
Legal	Itziar Sarasola	+34 XXX	Interpretazio legala
IT Lead	IT Officer	+34 XXX	Technical containment
Communications	CEO (Jon Zabala)	+34 XXX	Komunikazio kanpoa

---

7. AEPD JAKINARAZPEN CHECKLIST

- [ ] Urraketa detektatu da (data + ordua erregistratu)
- [ ] Berifikazio egina (false positive ez da)
- [ ] Impact assessment osatua (arrisku maila)
- [ ] DPO jakinarazi
- [ ] Breach response team aktibatu
- [ ] Containment neurri hartu (< 4h)
- [ ] AEPD web form bete (< 72h)

    - [ ] Urraketa deskribapena
    - [ ] Datu kategoriak eta kopurua
    - [ ] DPO kontaktu
    - [ ] Ondorio posibleak
    - [ ] Neurri adoptatu
- [ ] Afektatuei komunikatu (baldin arrisku altua) (< 72h)
- [ ] Txosten osoa AEPD bidali (< 72h)
- [ ] Forensic analysis hasi
- [ ] Lessons learned dokumentatu

---

8. POST-BREACH ACTIONS

8.1 Forensic Analysis

Arduraduna: CISO + Kanpoko aholkularitza **Timeline:** 1-2 asteak **Deliverable:** Forensic Report **Dokumentua:** `/security/forensics/reports/breach_YYYY-MM-DD_report.md`

8.2 Root Cause Analysis

Galderak:

- Nola sartu zen erasotzailea?
- Zer ahulezia ustatu zen?
- Zer kontrol falta zen?
- Nola ekiditu genezake etorkizunean?

8.3 Remediation Plan

Dokumentua: `/security/incidents/breach_remediation_plan.md`

Edukia:

- Gap analysis (zer falta zen)
- Neurri berri proposatu
- Budget eta timeline
- Responsible parties

8.4 Lessons Learned

Bilera: Breach Response Team + CGC **Timeline:** 2 asteko ondoren breach **Dokumentua:** `/security/incidents/lessons_learned_YYYY-MM-DD.md`

9. COMPLIANCE METRICS

KPI	Target	Egungo
Breach detection time	< 15 min	6h (⚠️ Hobetu)
Breach notification (AEPD)	< 72h	48h (✅)
Afektatuei notification	< 72h	72h (✅)
Containment time	< 4h	12h (⚠️ Hobetu)
Recovery time	< 24h	7 egun (❌ Hobetu)

Hobekuntza Plan: SOC 24/7 + EDR + SIEM

---

10. TRAINING

Maiztasuna: Bi-urteko **Audience:** Breach Response Team **Edukia:**

- RGPD Art. 33/34 interpretazioa
- Breach detection techniques
- Forensic analysis basics
- Crisis communication
- Tabletop exercise (breach simulation)

Hurrengo sesioa: 2026-06-15

---

11. ERREFERENTZIAK

- RGPD Art. 33-34
- WP29 Guidelines on Personal Data Breach Notification
- AEPD Guía Notificación Brechas
- `/security/incidents/sop_incident_response.md`
- `/compliance/gdpr/data_breach_notification_template.md`

ONARPENA: DPO (Ainhoa Uriarte) + CEO (Jon Zabala) - 2026-02-05 **HURRENGO BERRIKUSKETA:** 2027-02-05

Dokumentu hau sortu da RA4 (GDPR Aplikazioa) betebeharrak betetzeko, post-APT hobetuekin.