Conselleria de Famílies, Benestar
Social i Atenció a la Dependència
Direcció General d'Atenció a la Dependència
i Persones amb Discapacitat

COMUNICACIÓ A LES PERSONES AFECTADES PER LA VIOLACIÓ DE LA SEGURETAT DE DADES PERSONALS DEL SERVEI D'AJUDA A DOMICILI PER A PERSONES EN SITUACIÓ DE DEPENDÈNCIA GESTIONAT PER DOMUSVi

Per mitjà d'aquesta comunicació us informam que, com a conseqüència de l'accés no autoritzat d'un tercer als servidors de DOMUSVi que presta el servei d'ajuda a domicili (SAD) algunes de les vostres dades personals poden formar part d'un llistat de dades obtingut de manera il·lícita.

1. Dades de contacte del Delegat de Protecció de Dades de l'Administració de la CAIB:

protecciodades@dpd.caib.es

2. Punt de contacte en què es pot obtenir més informació:

a) Responsable del tractament: **Directora general d'Atenció a la dependència i Persones amb Discapacitat.**

responsabledades@dgad.caib.es

b) Encarregat del tractament: Servisar Servicios Sociales SLU (**DOMUSVi**)

Telèfon de contacte: **900 45 65 85.**
Delegat de Protecció de Dades (DPD): **dpo@domusvi.es**

3. Descripció general de l'incident i moment en què s'ha produït:

Com a conseqüència de l'accés no autoritzat a dades personals d'usuaris del SAD per part de terceres persones, el passat 10 de novembre de 2026 es va produir un incident de seguretat en els servidors de DOMUSVi que va comprometre la confidencialitat de les dades personals dels afectats.

4. Possibles conseqüències de la bretxa de dades personals:

Les possibles conseqüències d'aquesta bretxa de seguretat poden ser, entre d'altres:

a) Suplantació de la identitat.
b) Frau.
c) Pèrdua de privacitat i confidencialitat.
d) Danys en la reputació dels afectats.
e) Limitació dels seus drets.

5. Descripció de les dades i informació personal afectats:

Les dades personals a què s'ha tingut accés no autoritzat o il·lícit són les següents:

a) Nom i cognoms
b) Sexe
c) Document nacional d'identitat
d) Data de naixement
e) País i municipi de naixement i nacionalitat
f) Telèfon
g) Adreça domicili
h) Adreça de correu electrònic
i) Dades bancàries
j) Dades de salut

6. Resum de les mesures implantades fins ara per a controlar els possibles danys:

a) Bloquejar automàticament l'ordinador en què s'ha accedit a la base de dades exfiltrada
b) Canvi i reforç de totes les contrasenyes d'accés a les dades.
c) bloqueig de tots els usuaris relacionats amb l'actor sospitós.

7. Altres informacions útils als afectats perquè pugueu protegir les vostres dades o prevenir possibles danys:

a) Prestar especial atenció a possibles correus electrònics, missatges SMS, comunicacions a través d'aplicacions de missatgeria instantània o trucades telefòniques inesperades (Vishing) en què algú es faci passar per DOMUSVi, entitat d'ajuda a domicili, o per la Direcció General d'Atenció a la dependència i Persones amb Discapacitat, a fi d'obtenir informació personal o aconseguir que realitzi determinades accions.

b) Desconfieu de qualsevol comunicació en què se sol·licitin contrasenyes, codis d'accés, dades bancàries, documentació personal, informació sanitària o la realització de pagaments. No faciliteu aquest tipus d'informació mitjançant canals no verificats.

c) No obriu enllaços ni arxius adjunts sospitosos i comproveu l'autenticitat de qualsevol comunicació contactant directament amb DOMUSVi o amb la Direcció General d'Atenció a la Dependència i Persones amb Discapacitat a través dels seus canals oficials, sense utilitzar les dades de contacte incloses en el missatge rebut.

d) No faciliti informació personal, bancària o sanitària a persones la identitat i legitimitat de les quals no hagi pogut verificar, especialment si sol·liciten informació addicional sobre els serveis d'ajuda a domicili que rep o sobre les seves circumstàncies personals.

e) Reviseu periòdicament els moviments dels vostres comptes bancaris i targetes de crèdit o dèbit per detectar possibles operacions no autoritzades. Si observeu algun moviment sospitós, contacteu immediatament amb la vostra entitat bancària per comunicar-ho i sol·licitar les mesures de protecció oportunes.

f) Extremeu les precaucions davant de possibles intents de suplantació d'identitat i davant de qualsevol comunicació que utilitzi informació personal o sanitària per aparentar legitimitat o generar confiança.

g) Si teniu coneixement que les vostres contrasenyes o credencials d'accés poguessin haver-se vist compromeses, canvieu-les immediatament i, si utilitzeu les mateixes credencials en altres serveis, procediu també a modificar-les.

h) Conserveu qualsevol comunicació sospitosa que pugueu rebre i, en cas de detectar un possible ús fraudulent de les vostres dades personals o bancàries, comuniqueu-ho a les autoritats competents i a la Direcció general d'Atenció a la Dependència i Persones amb Discapacitat a través dels seus canals oficials.

Atentament,

Palma, en la data de la signatura electrònica
La directora general d'Atenció a la Dependència i Persones amb Discapacitat
Maria Castro Amor