ANNEX I. MESURES DE SEGURETAT REFORÇADES PER AL TRACTAMENT DE DADES SENSIBLES

1. Nivell de seguretat elevat

Atesa la naturalesa de les dades objecte del tractament, que inclouen categories especials de dades personals, l'ENCARREGAT es compromet a aplicar mesures tècniques i organitzatives de nivell alt, adequades al risc elevat per als drets i llibertats de les persones afectades.

2. Limitació estricta de l'accés

L'ENCARREGAT garantirà que:
a) L'accés a les dades sensibles sigui estrictament necessari per a la prestació del servei encarregat.
b) Només el personal expressament autoritzat i identificat tingui accés als sistemes i espais físics on es tracten aquestes dades.
c) Els perfils d'usuari siguin personalitzats, no compartits i revisats periòdicament.
d) Es disposi de mecanismes d'autenticació reforçada (com a mínim doble factor) per a l'accés als sistemes de tractament de les dades.

3. Registre i traçabilitat

L'ENCARREGAT mantindrà:
a) Registres detallats d'accés i operacions realitzades sobre les dades sensibles.
b) Sistemes de monitoratge que permetin detectar accessos anòmals o no autoritzats.
c) La conservació dels logs dels accessos als sistemes on es tractin les dades durant un període mínim de 6 mesos després de la finalització del servei, exclusivament amb finalitats de seguretat.

4. Deure reforçat de confidencialitat

L'ENCARREGAT garantirà que:
a) Tot el personal amb accés a dades hagi subscrit un compromís específic de confidencialitat.
b) El deure de secret subsisteixi indefinidament, fins i tot després de finalitzar la relació contractual o laboral.
c) Qualsevol vulneració del deure de confidencialitat sigui objecte de mesures disciplinàries internes.

5. Seguretat dels equips i suports

L'ENCARREGAT aplicarà, com a mínim, les mesures següents:
a) Xifrat de totes les dades sensibles emmagatzemades en servidors, equips o dispositius portàtils.
b) Prohibició d'emmagatzemar dades sensibles en dispositius personals o no autoritzats.
c) Protecció física dels equips mitjançant controls d'accés, sistemes d'alarma o mecanismes equivalents.

6. Seguretat de les comunicacions

L'ENCARREGAT garantirà que:
a) Tota transmissió de dades sensibles es realitzi mitjançant canals xifrats i segurs.
b) L'accés remot als sistemes de la fundació es faci exclusivament a través de VPN o mecanismes equivalents.
c) Es prohibeixi expressament l'ús de correu electrònic o serveis no autoritzats per transferir dades sensibles.

7. Còpies de seguretat i continuïtat

L'ENCARREGAT:
a) Realitzarà còpies de seguretat xifrades de les dades necessàries per garantir la recuperació davant incidents.
b) Mantindrà un pla de continuïtat i recuperació específic per a sistemes que tractin dades sensibles.
c) Verificarà periòdicament la integritat i la capacitat de restauració de les còpies.

8. Auditories reforçades

El RESPONSABLE tindrà dret a:
a) Sol·licitar evidències documentals de les mesures aplicades.
b) Realitzar auditories periòdiques, incloses auditories de seguretat, sobre els sistemes que tractin dades sensibles.
c) Exigir la correcció immediata de qualsevol deficiència detectada.