

## Qüestionari de Due Diligence per a encarregats de tractament

Aquest formulari s'ha desenvolupat per garantir que el Consorci Sanitari Integral compleixi amb el deure de diligència deguda abans de designar un proveïdor extern (encarregat del tractament de dades) i per ajudar a garantir que es fa una verificació adequada de la capacitat dels encarregats de tractament per assumir les responsabilitats de protecció de dades.

Si us plau, ompli el formulari responent a totes les preguntes amb el grau de detall adequat. Si teniu algun comentari o pregunta sobre les preguntes següents, poseu-vos en contacte amb [dpd@csi.cat](mailto:dpd@csi.cat)

Si us plau, intenteu proporcionar la vostra resposta, inclosa qualsevol documentació acreditativa.

| Qüestionari de Due Diligence |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| #                            | Preguntes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 1.                           | <b>Informació sobre el proveïdor:</b> <ul style="list-style-type: none"> <li>• <i>Rao Social:</i></li> <li>• <i>Adreça:</i></li> <li>• <i>NIF:</i></li> <li>• <i>Representant:</i></li> <li>• <i>DPD o contacte protecció de dades:</i></li> </ul>                                                                                                                                                                                                                                                                                                              |
| 2.                           | <b>Compliance Legal:</b> <p>2.1 <i>S'han dut a terme anteriorment avaluacions/auditories i/o revisions internes del compliment normatiu en matèria de protecció de dades? En cas afirmatiu, proporcioneu-ne una còpia.</i></p> <p>2.2 <i>Heu rebut alguna sol·licitud o consulta de l'Autoritat competent en matèria de Protecció de Dades? En cas afirmatiu, proporcioneu els detalls.</i></p> <p>2.3 <i>La vostra organització ha rebut alguna multa relacionada amb incidents de privacitat o seguretat? En cas afirmatiu, proporcioneu els detalls.</i></p> |
| 3.                           | <b>Polítiques i procediments formals:</b> <p>3.1 <i>S'han elaborat polítiques i procediments formals dins de l'àmbit de la protecció de dades? En cas afirmatiu, descriviu-los.</i></p> <p>3.2 <i>S'ha elaborat un Registre d'Activitats del Tractament (RAT) com a responsable i com a encarregat?</i></p> <p>3.3 <i>S'han dut a terme anàlisis de riscos i/o avaluacions d'impacte en protecció de dades?</i></p> <p>3.4 <i>Es revisen periòdicament aquests procediments i documents per tal d'assegurar-se que compleixen els requisits actuals?</i></p>    |
| 4.                           | <b>Confidencialitat:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>4.1 Les persones autoritzades per tractar dades personals del CSSV compleixen amb el deure de guardar la confidencialitat de la informació a la que accedeixen? Com es garanteix aquest compliment?</p>                                                                                                                                                                                                                                                                                                                                   |
| 5. | <p><b>Seguretat de la Informació i Gestió del Risc:</b></p> <p>5.1 S'ha adoptat algun marc de seguretat reconegut (per exemple, ISO 27001, NIST, etc.)?</p> <p>5.2 Disposeu d'una política de seguretat de la informació? En cas afirmatiu, cada quan es revisa.</p> <p>5.3 Disposeu d'un registre d'incidents de seguretat?</p> <p>5.4 Disposeu de personal intern o suport extern especialitzat en ciberseguretat?</p> <p>5.5 Disposeu d'una pòlissa de ciberseguretat?</p>                                                                |
| 6. | <p><b>Violacions de seguretat:</b></p> <p>6.1 Hi ha un procés formal aprovat per abordar les violacions de seguretat? Es revisa regularment?</p> <p>6.2 S'ha produït alguna violació de seguretat en els darrers 24 mesos? En cas afirmatiu, s'ha comunicat a l'Autoritat de Control? En cas afirmatiu, s'ha rebut resposta per part de l'Autoritat? Descriu els fets rellevants en relació al procediment seguit.</p>                                                                                                                       |
| 7. | <p><b>Cessió de dades amb tercers:</b></p> <p>7.1 Es realitzen cessions de dades a tercers?</p> <p>7.2 Treballeu amb proveïdors a qui s'hagin de cedir o hagin d'accedir a dades (subencarregats del tractament: emmagatzematge al núvol, etc.) En cas afirmatiu, indiqueu qui accedeix a les dades (incloent-hi el nom complet, la ubicació de l'empresa i l'activitat que realitza).</p> <p>7.3 En cas que disposeu de subencarregats de tractament, apliqueu un procediment formal d'avaluació de la diligència deguda dels mateixos?</p> |
| 8. | <p><b>Transferències Internacionals de Dades:</b></p> <p>8.1 Les dades es transfereixen i/o es tracten fora de l'Espai Econòmic Europeu (EEE)? En cas afirmatiu, aporteu informació sobre les TID: empresa o entitat a la que es cedeixen, mecanisme pel qual es fonamenta aquesta transferència, país de destí de les dades, etc.).</p>                                                                                                                                                                                                     |
| 9. | <p><b>Polítiques de conservació:</b></p> <p>9.1 Disposeu de polítiques de conservació i eliminació establertes per garantir que les dades s'eliminin de manera segura quan ja no siguin necessàries?</p> <p>9.2 Conserveu dades personals en format físic?</p>                                                                                                                                                                                                                                                                               |

|            |                                                                                                                                                                                                                                                                                                                                                                                         |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            |                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>10.</b> | <b>Formació per als professionals:</b><br><i>10.1 S'imparteix formació obligatòria en matèria de protecció de dades al personal? En cas afirmatiu, cada quant es realitza aquesta formació?</i><br><i>10.2 Es realitzen activitats de conscienciació sobre la protecció de dades i actualitzacions periòdiques sobre les novetats en la matèria (inforgrafies, recordatoris, etc.)?</i> |
|            |                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>11.</b> | <b>Drets dels interessats:</b><br><i>11.1 Disposeu d'un procediment de gestió de drets?</i><br><i>11.2 Quantes peticions d'exercici de drets heu rebut en els darrers 24 mesos? S'han resolt dins del termini màxim establert?</i>                                                                                                                                                      |
|            |                                                                                                                                                                                                                                                                                                                                                                                         |