

## RECOMANACIONS REFERENTS A LA PROTECCIÓ DE DADES PERSONALS

- Teletreballar des d'ordinadors "nets". En el cas que no siguin de la UAB assegurar que tenen un antivirus actualitzat així com el programari. No són recomanables ordinadors en els que els nens juguen, i que habitualment estaran "infectats". Cas d'estar infectats podrien "robar" les credencials d'accés i suplantar la nostra identitat, accedint a dades personals.
- Minimitzar la ubicació de dades personals en local, és a dir, fora dels repositoris corporatius (One Drive, Nebula, carpetes compartides, etc.). Si hi ha d'haver tractament en local, temporalitzar-lo, és a dir, fer-ho durant la tasca i, en acabar la tasca, retornar-les als repositoris corporatius i esborrar les dades locals.
- Reduir al mínim el tractament de dades de categories especials (salut, vida o orientació sexual, opinions polítiques, dades biomètriques o genètiques, etc...), i, si el tractament és imprescindible, evitar tractar-les en ubicacions locals.
- Bloquejar l'ordinador en abandonar-lo, especialment si s'estan tractant dades personals. Tot i ser un àmbit amb un nombre acotat de persones, els nens podrien posar en risc accidentalment la protecció de les dades personals.
- Si es fa alguna còpia, ha de ser en els repositoris corporatius. No són recomanables USB's o discos externs. Tampoc ho són altres ubicacions en el núvol que si no és amb credencials corporatives, per exemple un Dropbox personal.
- Davant de qualsevol tractament de dades personals, ser conscients del risc que comporta per als drets i llibertats de l'interessat, per exemple per la tipologia de dades, el volum d'afectats, la transmissió de les dades, etc.
- Minimitzar l'enviament de dades personals per correu electrònic i no utilitzar eines al núvol que no siguin les corporatives per enviar fitxers. En el cas de dades de categories especials encara més.
- En cas de produir-se un incident de protecció de dades (accessos no autoritzats, pèrdua d'informació, etc...) caldrà notificar-ho immediatament al delegat de protecció de dades ja que, si calgués comunicar-ho a l'Autoritat Catalana de Protecció de dades, el termini és de 72 hores segons RGPD / LOPDGDD.
- En el cas, no habitual, d'un desplaçament, el portàtil es podria perdre o ser robat. És a dir, vetllar per la seguretat física dels dispositius on hi poden haver dades personals.
- Tot i que quasi tota la informació estarà en suport digital, no descuidar la informació en paper, i si ja no és necessària caldrà destruir-la adequadament.

Bellaterra (Cerdanyola del Vallès), 23 de març de 2020



Xavier Rubiralta Costa  
Responsable tecnològic de protecció de dades

Agustí Verde Parera  
Delegat de protecció de dades