|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Medarbejders adfærd ift. GDPR** | **Gennemføres uge X** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at 2 udvalgte medarbejdere interviewes med spørgsmål herunder (se ideer til konkrete spørgsmål på sidste side) | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Når medarbejdere behandler personoplysninger, skal de som en naturlig del af deres adfærd sikre, at personoplysninger ikke deles med uvedkommende og generelt håndteres korrekt | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| Medarbejderen bekræfter, at mundtlig kommunikation med personoplysninger sker / er sket forsvarligt | | Har spurgt H og T, der hver for sig bekræfter, at evt. problematiske samtaler om og med borgere på områder i institutionen gennemføres, hvor ikke andre kan følge med i samtalen. | xx.xx.2025 |
| Medarbejderen bekræfter at lukke / låse til de lokaler som retningslinjer forskriver | | Har spurgt H og T, der hver for sig bekræfter, at de ved, hvilke døre der skal være lukket og/eller låst. De bekræfter begge, at de lukker og låser som foreskrevet. | xx.xx.2025 |
| Medarbejderen bekræfter, ikke at kende andre medarbejderes login og adgangskoder | | H bekræfter, at hun ikke er bekendt med andres adgangskoder.  T oplyser at en tidligere kollega havde adgangskode liggende på en seddel, men at adgangskoden ikke er anvendt af T. Problemstillingen giver anledning til tiltag nævnt herover. | xx.xx.2025 |
| Medarbejderen bekræfter at beskytte fortrolige og følsomme personoplysninger i daglige rutiner | | H fortæller, at hun fjerne informationer fra sit skrivebord ved arbejdstids ophør og låser kontordør, når kontor er ubemandet.  T oplyser, at hun som sådan ikke arbejder med fortrolige og følsomme oplysninger, men hvis disse modtages, gives de mundtligt videre til rette vedkommende. | xx.xx.2025 |
| Medarbejderen bekræfter, at private enheder (fx mobiltelefon) ikke anvendes til institutionens aktiviteter | | H og T bekræfter, at de ikke anvender private mobiltelefoner i arbejdstiden, men kun har disse fremme i pauser. | xx.xx.2025 |
| Medarbejderen bekræfter at låse PC og mobile enheder, når de forlades | | H bekræfter, at PC låses – jeg som leder har lagt mærke til, at PC er låst  T anvender ikke PC | xx.xx.2025 |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Medarbejders viden om GDPR** | **Gennemføres uge X** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at 2 udvalgte medarbejdere skriftligt besvarer spørgsmål (fx ved at stille spørgsmål med flere svarmuligheder), der skal afdække deres viden om GDPR (se ideer til konkrete spørgsmål på sidste side) | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Når medarbejdere arbejder med personoplysninger, skal de have en forståelse for, at personoplysninger skal behandles med omtanke og efter reglerne | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| At medarbejdere har en tilstrækkelig viden om hvordan personoplysninger håndteres korrekt.  Fx at der kun må indsamles personoplysninger, der er relevante for at løse opgaven, og at mundtlig kommunikation skal ske under hensyn til at evt. uvedkommendes kan lytte med | | Anvendt DPO’s spørgeramme – se sidste side. På personalemøde har alle medarbejdere anonymt svaret på spørgsmål.  På nær hos en enkelt medarbejder, viser besvarelsen at alle har en tilstrækkelig viden.  Problemstillingen giver anledning til tiltag nævnt herover. | xx.xx.2025 |
| At medarbejdere har en nødvendig viden om at omfanget af data bør minimeres  Fx at der kun sker opbevaring af personoplysninger, hvis det har et formål og at det er nødvendigt løbende at slette personoplysninger | | Anvendt DPO’s spørgeramme – se sidste side. På personalemøde har alle medarbejdere anonymt svaret på spørgsmål.  Besvarelsen viser at alle har en tilstrækkelig viden. | xx.xx.2025 |
| At medarbejderen kender kontaktpersoner, hvis der er spørgsmål til GDPR-forhold herunder spørgsmål fra de registrerede borgere mv. | | Anvendt DPO’s spørgeramme – se sidste side. På personalemøde har alle medarbejdere anonymt svaret på spørgsmål.  Besvarelsen viser at alle ved at leder eller GDPR-kontaktperson skal kontaktes og vil håndtere evt. spørgsmål | xx.xx.2025 |
| At medarbejderen kan identificere persondatabrud / sikkerhedsbrud | | Anvendt DPO’s spørgeramme – se sidste side. På personalemøde har alle medarbejdere anonymt svaret på spørgsmål.  Besvarelsen viser at der er tvivl om hvad der er persondatabrud Problemstillingen giver anledning til tiltag nævnt herover. | xx.xx.2025 |
| At medarbejderen kender den person der skal kontaktes ved persondatabrud | | Anvendt DPO’s spørgeramme – se sidste side. På personalemøde har alle medarbejdere anonymt svaret på spørgsmål.  Besvarelsen viser at alle ved at leder skal kontaktes ved persondatabrud | xx.xx.2025 |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Fysiske forhold i institutionens lokaler** | **Gennemføres uge X** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at lave en fysisk gennemgang af lokaler herunder de fysiske forhold fx adgangsmuligheder, låse, skabe mv. | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Behandling af personoplysninger skal ske med tilstrækkelige fysiske foranstaltninger, der sikrer en god beskyttelse af personoplysninger | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| At det kun er relevante personoplysninger, der er synlige på institutionens fællesarealer (fx på opslagstavler, whiteboards mv.) og at informationerne som udgangspunkt kun er tilgængelige for dem det vedrører | | Der er foretaget en fysisk gennemgang af alle lokaler, og der er ikke fundet personoplysninger der ikke burde være tilgængelige. | xx.xx.2025 |
| Tag 2 stikprøver på, at medarbejdere ikke opbevarer brugernavn og adgangskode skriftligt fx på fysisk papir, eller er noteret på en måde / på et medie hvor informationerne kan være tilgængelige for andre | | Der er foretaget en fysisk gennemgang af arbejdspladser og tilsvarende mhp. at efterse, om der findes nedskrevne adgangskoder.  Alt var tilfredsstillende | xx.xx.2025 |
| Det kontrolleres, at skabe og kontorer er låst, at skriveborde er ryddet, at mapper med personoplysninger er opbevaret jf. retningslinjer og med særlig fokus på at fortrolige og følsomme personoplysninger er skærmet for uvedkommende | | På tidspunkter hvor arbejdspladser og relevante lokaler var ubemandet, er der foretaget en gennemgang af, at personoplysninger ikke er opbevaret tilgængeligt for uvedkommende, at PC skærme ikke er uhensigtsmæssigt placeret og døre er låst osv.  Alt var tilfredsstillende | xx.xx.2025 |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Personoplysninger på fysiske dokumenter** | **Gennemføres uge X** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at lave en gennemgang af fysiske dokumenter / noter mv., uanset hvor de befinder sig, og uanset hvad baggrunden er for, at de findes. | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Personoplysninger (og særligt fortrolige og følsomme personoplysninger), der findes på fysiske dokumenter / noter mv. skal beskyttes, så de ikke kommer til uvedkommendes kendskab | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| Tag 2 stikprøver på, at midlertidigt registrerede personoplysninger på fysiske dokumenter (fx notater, referater, løse noter, dokumenter til arkivering eller lignende) er opbevaret sikkert | | Der er taget 2 stikprøver hos xx, hvor noter, post-its og arkiverings-bunken er undersøgt. Alle dokumenter har haft et formål og er opbevaret tilfredsstillende, dvs. utilgængeligt for uvedkommende | xx.xx.2025 |
| Tag 2 stikprøver på, at der ikke forefindes fysiske dokumenter (fx notater, referater, løse noter, dokumenter til arkivering eller lignende) med personoplysninger, der burde være registreret i fagsystemer | | Der er tage 2 stikprøver af mødereferater og dokumenter, og det er efterset, at de informationer der bør systemregistreres, også er registreret i vores primære system xx.  Alt var tilfredsstillende | xx.xx.2025 |
| Tag 2 stikprøver på, at der ikke forefindes fysiske dokumenter (fx notater, referater, løse noter, dokumenter til arkivering eller lignende) med personoplysninger der burde være slettet/tilintetgjort jf. fastlagte sletteregler | | Der er udvalgt 2 fysiske dokumenter, og det kunne konstateres, at de pågældende dokumenter burde være makuleret. | xx.xx.2025 |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Personoplysninger i systemer / enheder** | **Gennemføres uge X** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at gennemgå indholdet af personoplysninger i it- / fagsystemer og it-enheder | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Personoplysninger bør registreres og håndteres i it-systemer med den bedste databeskyttelse i forhold til typen af oplysning.  Personoplysninger skal slettes fra it-systemer og it-enheder, når der ikke er et lovligt formål med at opbevare oplysningerne længere | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| Tag 2 stikprøver af, at der ikke registreres flere personoplysninger end det er nødvendigt for at institutionen kan løfte sine bundne opgaver. | | 2 underretninger er gennemgået, og det er kontrolleret, at der ikke er registreret oplysninger, der ikke har relevans for sagsbehandlingen.  Alt var tilfredsstillende | xx.xx.2025 |
| Tag 2 stikprøver af, at der ikke er opbevaret personoplysninger (sager) i længere tid end der er et lovligt formål hermed (jf. fastlagt slettefrister) | | Det er ved 2 stikprøver kontrolleret, at hhv. personalesager og afdelingens mødereferater er slettet jf. slettefrist.  Alt var tilfredsstillende | xx.xx.2025 |
| Tag 2 stikprøver af, at nye og gamle billeder kun opbevares / er slettet som anført i institutionens retningslinjer | | Det er undersøgt, at billeder, der er opbevaret på institutionens enheder, ikke er over x måneder gamle, som fremgår af vores sletteregler.  Alt var tilfredsstillende | xx.xx.2025 |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Billeder og kommunikation med borger** | **Gennemføres uge** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at gennemgå de enkelte kommunikationsområder, og undersøge hvorvidt interne retningslinjer for kommunikation med personoplysninger er overholdt | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Samtykke skal være overholdt, og den skriftlige kommunikation med personoplysninger skal ske på en sikker måde og kun med rette vedkommende | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| Find de evt. personer hvor der **ikke** er givet samtykke til offentliggørelse af billeder på (fx sociale medier, hjemmesider mv) og kontroller, at der ikke findes billeder af disse personer | | Ikke relevant, da vi ikke anvender GDPR-samtykke som grundlag for behandlingen af personoplysninger | xx.xx.2025 |
| Det kontrolleres, at personer på offentliggjorte billeder (uanset hvor de er offentliggjort) ikke burde føle sig krænket | | 2 beboere er adspurgt, om de billeder der er taget af dem og vist i månedsbladet er ok – dvs. de føler sig ikke krænket i de givne situationer.  Alt var tilfredsstillende | xx.xx.2025 |
| Tag 2 stikprøver af mails fra den ”ikke sikre mailboks”, og kontroller, at der ikke er omfattet fortrolige og følsomme oplysninger | | Vi har kun sikker mailboks, leveret af KK.  Der er taget to stikprøver på mailkorrespondance der potentielt kunne indeholde personoplysninger. Der var personoplysninger med det var alene almindelige oplysninger, de følsomme forhold og oplysninger var kommunikeret via e-boks. | xx.xx.2025 |
| Tag 2 stikprøver af mails med fortrolige og følsomme oplysninger og kontroller at de er sendt til korrekt modtager | | Vi udveksler generelt ikke fortrolige og følsomme oplysninger pr. mail  Der er dog taget 2 stikprøver af mails, der potentielt kunne indeholde fortrolige eller følsomme oplysninger fordi emnet var xxx. Der var ingen sådanne oplysninger i disse mails. | xx.xx.2025 |
| Det kontrolleres, at evt. skriftlig kommunikation (ml. borger og institution) gennem andet end via mail ikke indeholder personoplysninger. Det kunne fx være gennem SMS | | Med den borgergruppe, hvor SMS er nødvendig at anvende som kommunikationsvej, er der hos C og P medarbejder taget stikprøver på, at der ikke er angivet personoplysninger.  Alt var tilfredsstillende | xx.xx.2025 |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Borgers/medarbejderes (registreret) rettigheder** | **Gennemføres uge** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at spørge relevante personer og eller undersøge registreringer / gemte mailbesvarelser. | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  At borgere og medarbejdere (registrerede) skal grundlæggende være oplyst om indhold og omfang af de behandlinger, der fortages af institutionen (oplysningspligt). Desuden skal de registrerede have besvaret løbende spørgsmål til institutionens behandling af den registreredes oplysninger. | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| Tag 2 stikprøver af, at medarbejdere har modtaget privatlivspolitik ved ansættelsen fx ved at spørge medarbejderen om de har set politikken. | | A og K, der er de sidst ansatte på institutionen, har bekræftet, at de har modtaget / set privatlivspolitik. | xx.xx.2025 |
| Tag 2 stikprøver på, at borgere har modtaget privatlivspolitik ved ankomst til institutionen fx ved at spørger borgeren om de har set politikken. | | Der er taget stikprøver hos 2 beboer på gang 4, der bekræfter, at de har modtaget privatlivspolitik. Dog oplyser den ene beboer, at vedkommende ikke har læst den, men beboer er opmærksom på indholdet. | xx.xx.2025 |
| Tag 2 stikprøver på at borgeres henvendelser om ændringer til egne personoplysninger har medført korrekte ændringer i institutionens registreringer (fx adresseændring, personlige oplysninger etc) | | Der har ikke været nogen henvendelser siden sidste kontrol. | xx.xx.2025 |
| Undersøg om borgere har henvendt sig med spørgsmål egne oplysninger og undersøg om henvender har modtaget svar. (hvis muligt 2 stikprøver) fx ved at undersøge mailbesvarelse eller spørge henvender. | | Der har siden sidste kontrol været én mundtlig henvendelse til en medarbejder om, hvem der var angivet som nærmeste pårørende. Henvendelsen er givet videre til adm. medarbejder, har undersøgt registreringer om nærmeste pårørende. Registreringerne var korrekte hvilket er bekræftet overfor borger. | xx.xx.2025 |

**SPØRGERAMME**

|  |  |
| --- | --- |
| **EMNE - VIDEN** | **IDEER TIL SPØRGSMÅL – (**spørgsmål med flere svarmuligheder) |
| At medarbejdere generelt har en tilstrækkelig viden om korrekt håndtering af personoplysninger | Hvad er korrekt håndtering af personoplysninger  Oplysninger indsamles for at løse en driftsopgave (korrekt)  Oplysninger gemmes fordi de er rare at have, hvis de måske skal bruges igen (ikke korrekt)  Samme oplysninger opbevares på papir og i system for en sikkerheds skyld (ikke korrekt)  Oplysninger kan uden problemer sendes til anden institution (Ikke korrekt)  Kommunikation med personoplysninger skal ske uden at uvedkommende kan følge med (korrekt) |
| At medarbejdere har en nødvendig viden om betydning af dataminimering | Hvad betyder det at dataminimerer:  At der indsamledes så mange personoplysninger som muligt for at være sikker (ikke korrekt)  At personoplysning kun opbevares hvis det er et krav (korrekt)  At dokumenter / sager med personoplysninger løbende skal slettes (korrekt)  At det er nødvendigt at gemme alle billeder der er taget (ikke korrekt) |
| At medarbejderen kender kontaktpersoner, hvis der er spørgsmål til GDPR-forhold herunder spørgsmål fra de registrerede borgere mv. | Hvem i institutionen skal du kontakte, hvis en borger har spørgsmål til de personoplysninger, som i har om vedkommende? |
| At medarbejderen kan identificere persondatabrud / sikkerhedsbrud | Giv 3 eksempler på hændelser, der muligvis kan anses som et databrud eller et sikkerhedsbrud? |
| At medarbejderen kender den person, der skal kontaktes ved persondatabrud | Hvem i institutionen skal du kontakte, hvis du har opdaget noget, der kunne være et databrud eller et sikkerhedsbrud? |