DEPARTAMENTUL DE STUDII PARLAMENTARE ȘI POLITICI UE

DIRECȚIA STUDII ȘI DOCUMENTARE LEGISLATIVĂ

CERINȚE LEGALE APLICABILE PORTALURILOR INSTANȚELEOR DE JUDECATĂ, ÎN STATELE MEMBRE ALE UNIUNII EUROPENE

OCTOMBRIE 2018

Documentare şi sinteză: Alina Bragagiu, consilier parlamentar

* Lucrarea poate fi accesată direct pe Intranet la pagina Direcţiei studii şi documentare legislativă

C U P R I N S

INTRODUCERE[1]

Cerințe legale pentru website-uri în Uniunea Europeană[2] aplicabile și portalurilor instanțelor de judecată:

Conținutul publicat în Europa - versiunile online ale documentelor oficiale sau conținutul adaptat pe Web - trebuie să îndeplinească anumite cerințe legale: Anunțurile legale și drepturile de autor sunt întotdeauna necesare; Cookie-urile necesită consimțământ informat; Disclimer pentru conținutul adaptat Web pentru a declara responsabilitatea în UE; Comunicarea privind protecția datelor care explică în mod explicit modul în care vor fi utilizate toate informațiile personale colectate de la utilizatori; Toate paginile trebuie să respecte Regulile pentru conținut Web (WCAG) 2.0, nivel AA.

Sinteză privind Directiva (UE) 2016/680 – protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile polițienești și judiciare din sectorul penal și privind libera circulație a acestor date. Directiva înlocuiește Decizia-cadru 2008/977/JAI privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală începând cu 6 mai 2018[3]

Directiva impune ca datele colectate de autoritățile de aplicare a legii să fie: prelucrate în mod legal și echitabil; colectate în scopuri determinate, explicite și legitime și să fie prelucrate numai potrivit acestor scopuri; adecvate, relevante și neexcesive în ceea ce privește scopurile în care sunt prelucrate; exacte și actualizate dacă este necesar; păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele respective; securizate adecvat, incluzând protecția împotriva prelucrării neautorizate sau ilegale.

Directiva impune ca autoritățile de aplicare a legii să facă o distincție clară între datele diferitelor categorii de persoane, inclusiv: cele în privința cărora există motive serioase să se creadă că au săvârșit sau că urmează să săvârșească o infracțiune; cele care au fost condamnate pentru săvârșirea unei infracțiuni; victimele unor infracțiuni sau persoanele în privința cărora există motive să se creadă că ar putea fi victimele unor infracțiuni; cele care sunt părți care au legătură cu infracțiunea, inclusiv potențialii martori.

Persoanele fizice au dreptul să li se pună la dispoziție anumite informații de către autoritățile de aplicare a legii (mai precis, de protecție a datelor), inclusiv: numele și datele de contact ale autorității competente care hotărăște scopul și mijloacele de prelucrare a datelor; scopurile prelucrării datelor lor; dreptul de a depune o plângere la

[1] https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/
[2] http://ec.europa.eu/ipg/basics/legal/index_en.htm
[3] https://eur-lex.europa.eu/content/news/guidance-for-general-data-protection-regulation-application.html

o autoritate de supraveghere și datele de contact ale autorității; existența dreptului de a solicita accesul și corectarea sau ștergerea datelor proprii cu caracter personal, cât și dreptul de a restricționa prelucrarea datelor proprii cu caracter personal.

Autoritățile naționale trebuie să ia măsuri tehnice și organizatorice pentru a asigura un nivel de securitate pentru datele cu caracter personal care să fie corespunzător acestui risc. În cazul în care prelucrarea datelor este automată, trebuie aplicate câteva măsuri, inclusiv: împiedicarea accesului persoanelor neautorizate la echipamentele utilizate pentru prelucrare; împiedicarea oricărei citiri, copieri, modificări sau eliminări neautorizate a suporturilor de date; împiedicarea introducerii neautorizate de date cu caracter personal și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal stocate.

Președinția Consiliului UE a publicat un proiect revizuit al regulamentului privind confidențialitatea în mediul electronic, la 20 septembrie 2018.[4]

Printre mențiunile făcute: Articolul 7 din Carta Drepturilor Fundamentale a Uniunii Europene ("Carta") protejează dreptul fundamental al fiecăruia la respectarea vieții private și de familie, a locuinței și a comunicațiilor. Respectarea confidențialității comunicărilor este o dimensiune esențială a acestui drept, aplicată atât persoanelor fizice, cât și persoanelor juridice.

Confidențialitatea comunicațiilor electronice asigură faptul că informațiile schimbate între părți și elementele externe ale unei astfel de comunicări, inclusiv atunci când informațiile au fost trimise, (de unde, către cine,) nu trebuie dezvăluite nimănui decât părților implicate într-o comunicare. Principiul confidențialității ar trebui să se aplice mijloacelor de comunicare actuale și viitoare, inclusiv apeluri, acces la internet, aplicații de mesagerie instant, e-mail, apeluri telefonice prin internet și mesaje personale furnizate prin intermediul rețelelor sociale.

Datele privind comunicațiile electronice pot dezvălui, de asemenea, informații referitoare la persoane juridice, cum ar fi secrete de afaceri sau alte informații sensibile cu valoare economică și a căror protecție permite persoanelor juridice să-și desfășoare activitatea, sprijinind, printre altele, inovarea. Prin urmare, dispozițiile prezentului regulament ar trebui, în principiu, să se aplice atât persoanelor fizice, cât și persoanelor juridice. În plus, prezentul regulament ar trebui să se asigure că, dacă este necesar, dispozițiile Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului se aplică mutatis mutandis și utilizatorilor finali care sunt persoane juridice.

Prezentul regulament nu ar trebui să se aplice in defavoarea protecției drepturilor și libertăților fundamentale privind activitățile legate de securitatea și apărarea națională.

[4] https://iapp.org/media/pdf/resource_center/ePrivacyReg-2018-09-20-draft.pdf

Personal imput:

Portalurile de judecată din statele membre respectă principiile prevăzute de Regulamentul general privind protecția datelor UE 679/2016, în special prin reducerea la minimum a datelor, respectând principiului integrității și confidențialității, folosesc anonimzarea, informațiile sunt prezentate într-o formă care să nu poată permite identificarea persoanei; pseudonimizarea, oferind nume de dosar și termeni clasici reclamant, reclamat, etc; accesul la informații este oferit doar anumitor persoane prin user și parolă.

Instanțele statelor membre ale Uniunii Europene (UE) aplică și interpretează legea națională, precum și legislația UE. Prin urmare, este în interesul cetățenilor și al juriștilor să aibă acces nu numai la jurisprudența propriului stat membru, ci și la cea a altor state membre ale UE.[5] Pot fi consultate mai multe situații și observate tehnicile GDPR implementate.

Transpunerile legilor în statele membre UE cu privire la Regulamentul UE 679/2016 nu au conținut specific pentru portalurile instanțelor de judecată, ori pentru oricare alt tip de website.

Transpunerea reglementărilor europene în legislația națională[6]

Transpunerea in Romania[7]

Legea Nr.190/2018

Art. 6. - Prelucrarea datelor cu caracter personal și de categorii speciale de date cu caracter personal, în contextul îndeplinirii unei sarcini care servește unui interes public

În cazul în care prelucrarea datelor personale și speciale este necesară pentru îndeplinirea unei sarcini care servește unui interes public conform art. 6 alin. (1) lit. e) *(prelucrarea este necesaă pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul;)* și art. 9 lit. g) (*prelucrarea este necesara din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor*

[5] https://e-justice.europa.eu/content_member_state_case_law-13-en.do
[6] https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/

[7] https://www.senat.ro/legis/PDF/2018/18L294FP.pdf

persoanei vizate;) din Regulamentul general privind protecția datelor se efectuează cu instituirea de către operator sau de către partea terță a următoarelor garanții:

a) punerea în aplicare a măsurilor tehnice și organizatorice adecvate pentru respectarea principiilor enumerate la art. 5 din Regulamentul general privind protecția datelor, în special a reducerii la minimum a datelor, respectiv a principiului integrității și confidențialității;

b) numirea unui responsabil pentru protecția datelor, dacă aceasta este necesară în conformitate cu art. 10 din prezenta lege;

c) stabilirea de termene de stocare în funcție de natura datelor și scopul prelucrării, precum și de termene specifice în care datele cu caracter personal trebuie șterse sau revizuite în vederea ștergerii.

Art. 10 Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni. Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe în temeiul articolului 6 alineatul (1) se efectuează numai sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii Europene sau de dreptul intern care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat.

”GDPR Expert Insights”[8] cuprinde cinci secțiuni pentru a ajuta organizațiile să implementeze și să respecte prevederile Regulamentului UE privind protecția generală a datelor. Prima secțiune, un articol intitulat "Primul pas privind raportarea încălcărilor datelor cu caracter personal în conformitate cu Regulamentul general al Uniunii Europene privind protecția datelor", descrie raportarea privind încălcarea datelor cu caracter personal de către procesatorii de date și controlorii de date în cadrul GDPR. Lista de verificare a programului GDPR oferă zece etape ajutătoare pentru a vă alinia programul de confidențialitate cu GDPR.

AUSTRIA

Austria este a doua țară UE după ce Germania a adoptat o nouă lege națională[9] privind protecția datelor ("Legea nouă") care implementează GDPR. Noul act, publicat oficial la 31 iulie 2017, va modifica actualele legi privind protecția datelor și va deveni aplicabil în același timp cu GDPR.

[8] https://iapp.org/media/pdf/resource_center/EU-GDPR-Practical-Guidance_final.pdf
[9] https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html

Spre deosebire de actul de punere în aplicare GDPR în Germania, Noul Act este relativ rezervat în adăugarea de variații naționale. Principalele puncte care au legătura cu subiectul acestui studiu ale noului Act austriac sunt:

Aplicarea pentru persoanele juridice. Așa cum se întâmplă și în prezent în legislația austriacă referitoare la confidențialitate, dreptul fundamental la confidențialitatea datelor se va aplica în Austria nu numai persoanelor fizice, ci și persoanelor juridice. Prin contrast, GDPR și cele mai multe legi naționale privind confidențialitatea UE se aplică numai informațiilor personale referitoare la persoanele fizice.

Prelucrarea informațiilor privind condamnările penale și infracțiunile de către entități private. Articolul 10 din GDPR prevede că informațiile privind condamnările penale și infracțiunile pot fi prelucrate numai dacă sunt autorizate de legislația statelor membre. Punctul 4, secțiunea 3 din Noul Act prevede această posibilitate în Austria. Pe lângă o referire generală la prelucrarea unor astfel de informații în temeiul unei autorizații sau al unei obligații legale, Noul Act indică, de asemenea, că aceste informații pot fi prelucrate, dacă este necesar, în scopul intereselor legitime (în sensul articolului 6 alineatul (1) litera (f) GDPR). Aceasta este o posibilitate distinctă pe care nu am văzut-o încă în alte acte de punere în aplicare și care ar schimba în mod semnificativ restricția introdusă prin articolul 10 din GDPR.

Repertoriul legislativ (tradus în limba engleză) poate fi consultat pe website-ul Ministerului Federal pentru Digitizare și Afaceri Locale.[10]

BELGIA

La 5 septembrie 2018 Belgia a publicat legea de punere în aplicare a aspectelor de fond ale Regulamentului UE privind protecția generală a datelor. În special, legea abordează diferitele domenii de divergență națională permise de GDPR. În consecință, cadrul juridic belgian pentru protecția datelor este acum complet și constă, în esență, în următoarele:

"Legea instituțională" (Legea din 3 decembrie 2017 de instituire a Autorității pentru Protecția Datelor); "Legea fundamentală[11]" (Legea din 30 iulie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor personale); "Legea privind recursul colectiv" (Legea din 30 iulie 2018, cu diverse dispoziții în materie economică, care introduce acțiuni colective în despăgubire); "Legea securității informațiilor" (Legea din 5 septembrie 2018 privind crearea unui Comitet pentru

[10] https://www.ris.bka.gv.at/Ergebnis.wxe?Abfrage=Erv&Titel=&Quelle=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=EinemJahr&ResultPageSize=100&Suchworte=Protection+of+Personal+Data&Position=1

[11] https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/09/20180730-Belgian-law.pdf

Securitatea Informațiilor); și " Legea camerelor de supraveghere" (Legea din 21 martie 2018 de modificare a Legii din 21 martie 2017 privind instalarea și utilizarea camerelor de supraveghere).

Prelucrarea de către autoritățile publice a anumitor infracțiuni (articolul 83.7 GDPR): Legea fundamentală pune în aplicare, de asemenea, Directiva 2016/680 / UE privind prelucrarea datelor cu privire la infracțiunea penală și reglementează astfel prelucrarea datelor cu caracter personal de către autoritățile publice, autoritățile vamale. De asemenea, aceasta scutește toate autoritățile publice de amenzi impuse de Autoritatea pentru Protecția Datelor. În plus, restricțiile prevăzute de Legea IFC se referă la amploarea drepturilor persoanelor vizate în legătură cu autoritățile publice care efectuează investigații (taxe, comerț etc.).[12]

De menționat că în conformitate cu articolul 10 din GDPR, prelucrarea datelor cu caracter personal referitoare la condamnările penale și infracțiunile sau măsurile de securitate aferente în temeiul articolului 6 alineatul (1) poate fi efectuată numai sub controlul autorității publice sau atunci când prelucrarea este autorizată de Uniune sau Legislația statelor membre care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate. Actul de punere în aplicare a GDPR prevede un număr limitat de motive juridice pentru prelucrarea datelor privind condamnările penale, impune condiții suplimentare și introduce măsuri specifice de securitate pentru prelucrarea acestora.

Datele privind condamnările penale pot fi procesate: de către întreprinderi private, dacă este necesar pentru gestionarea litigiilor la care sunt parte; de către avocați sau alți consilieri juridici, în măsura necesară pentru apărarea intereselor clienților săi; de către alte persoane, atunci când prelucrarea este necesară pentru îndeplinirea scopurilor stabilite de sau în temeiul unei legi; și dacă este necesar în scopuri de arhivare, cercetare științifică sau istorică sau scopuri statistice.

Acoperirea Legii fundamentale reflectă articolul 3 din GDPR cu privire la domeniul teritorial. În acest sens, Legea fundamentală se aplică activităților unui operator sau unui prelucrator stabilit (i) în Belgia sau (ii) în afara Uniunii Europene, dar care procesează date referitoare la persoane fizice situate în Belgia (cu condiția să ofere, de asemenea, bunuri sau servicii sau care face profilare în Belgia).

Legea Camerelor de supraveghere, modificată în 2018, a transferat obligația de a notifica utilizarea și instalarea camerelor de la DPA la CSAM (Inițiativă Comună A Serviciilor Guvernamentale) prin intermediul site-ului www.declarationcamera.be. În plus, în conformitate cu cerințele GDPR, Legea Camerelor de supraveghere pune în aplicare obligațiile de a menține un registru, de a efectua o evaluare a impactului, de a desemna un DPO și de a respecta drepturile persoanelor vizate.

[12] https://iapp.org/news/a/belgium-finalizes-gdpr-implementation-a-practitioners-view/

Pentru unele jurisdicții, este posibil să utilizați numărul de rol sau data pentru a afla starea cazului dvs. (caz nou, în curs de desfășurare sau livrat). Pentru a face acest lucru, trebuie să consultați secțiunea "fișierul dvs.", care se găsește de obicei în dreptunghiul portocaliu al jurisdicției în cauză (cu condiția ca această funcționalitate să fie operațională).

Instanțe de judecată[13], jurisdicția în ordine alfabetică[14]

CROAȚIA

Legea croată privind punerea în aplicare a Regulamentului general privind protecția datelor[15] a fost adoptată la 27 aprilie 2018, publicată oficial la 3 mai și a intrat în vigoare la 25 mai.

Legea reglementează componența autorităților de supraveghere, autoritățile și principiile muncii, precum și particularitățile legate de amenzile administrative și procedurile în fața autorității de supraveghere și a instanțelor administrative. Legea prevede, de asemenea, unele prevederi specifice legate de prelucrarea datelor genetice și biometrice, supravegherea video, informațiile despre minori și prelucrarea datelor în scopuri statistice. În opoziție cu Legea privind protecția datelor cu caracter personal, care a fost pusă în aplicare pentru a atinge obiectivele stabilite de Directiva 95/46 / EZ, legea actuală nu prevede dispoziții specifice referitoare la Data Protection Officer. De asemenea, nu mai există o dispoziție potrivit căreia datele puse la dispoziția publicului de către persoana vizată reprezintă baza legală de prelucrare în sine.

Ca o particularitate națională, Legea prevede o derogare de la articolul 9 alineatul (2) litera (a) din GDPR, în cazul în care categoria specială de date cu caracter personal nu poate fi procesată în niciun caz, nici măcar pe baza consimțământului expres al subiectului datelor. Aceasta se referă la prelucrarea datelor genetice în scopul calculării probabilității de apariție a bolii sau a altor aspecte de sănătate ale persoanelor vizate în cadrul activităților legate de încheierea sau executarea contractelor de asigurare de viață. De menționat și că organele administrației de stat, alte organe de stat și unitățile de autoguvernare locală și regională sunt excluse din aplicarea amenzilor administrative.

[13] https://dossier.just.fgov.be/fr/
[14] https://www.tribunaux-rechtbanken.be/sites/default/files/public/content/uwdossiervolgensgemeente_0.pdf
[15] https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_05_42_805.html

DANEMARCA

Scopul acestui act[16] a fost de a implementa GDPR în legislația daneză și niciun membru al Parlamentului nu a votat împotriva sa. Dar, Legea privind protecția datelor din Danemarca a întâmpinat opoziție din partea diferitelor organizații datorită faptului că actul permite autorităților publice să utilizeze datele personale ale persoanelor fizice într-un alt scop decât cel pentru care au fost colectate datele inițiale.

Amenzile către autoritățile publice. Este posibil să se impună amenzi autorităților publice. Comentariile explicative la proiectul de lege presupun o amendă maximă de 4% din subvenția de funcționare a autorității publice, cu toate acestea nu mai mult de 16 milioane DKK.

Cerințele din vechiul Act privind aprobarea prealabilă din partea Agenției daneze pentru protecția datelor cu privire la utilizarea registrelor de avertizare, a agențiilor de rating de credit și a sistemelor de informații judiciare sunt reintroduse.

Totodată, se reintroduc regulile existente privind prelucrarea datelor cu caracter personal în cadrul administrării personalului. Legea daneză privind protecția datelor completează GDPR, permițând prelucrarea datelor sensibile în cursul administrării personalului pe baza intereselor legitime. De asemenea, regula se aplică și autorităților publice, ceea ce este demn de remarcat, deoarece autoritățile publice nu pot folosi temeiul juridic "interes legitim" în GDPR.

În plus, legea stabilește că se poate folosi consimțământul ca bază legală pentru prelucrarea datelor HR. Astfel, legea extinde avizul Departamentului de Justiție al Danemarcei în raportul lor privind GDPR; un aviz contrar grupului de lucru al articolului 29, care, în numeroase ocazii, a pus la îndoială utilizarea consimțământului în raporturile de muncă.

Legea daneză privind protecția datelor deschide calea, după negocierea cu ministrul justiției, pentru prelucrarea datelor cu caracter personal de autoritățile publice în alte scopuri decât cele pentru care acestea au fost inițial colectate.

Mai mult, obligațiile de transparență ale autorităților publice sunt limitate atunci când are loc o prelucrare pentru un nou scop, dat fiind că persoana vizată în această situație nu are dreptul să primească informații despre prelucrare pentru un astfel de scop nou. Cu toate acestea, excepția nu se aplică în măsura în care scopul prelucrării este alinierea sau combinarea datelor cu caracter personal în scopul controlului.

[16] https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf

ESTONIA

La 5 iunie 2018, Parlamentul a acceptat un proiect de lege[17] pentru punerea în aplicare a Directivei privind protecția datelor cu caracter personal. Acest proiect de lege modifică 130 de legi estoniene pentru a se asigura că sunt conforme cu GDPR. În prezent, nu este cunoscut când va fi trecut acest proiect de lege. Informația a fost preluată de pe EIS, un mediu de lucru în care se desfășoară coordonarea interdepartamentală a documentelor, transmiterea către guvern și Riigikogu, precum și consultarea publică. Această pagină a fost updatată la 18.08.2018.

FINLANDA

Procesul legislativ în legătură cu GDPR este încă în desfășurare în Finlanda. La 1 martie 2018, guvernul și-a prezentat propunerea de abrogare a actualei legi privind datele personale (523/1999) și o înlocuiește cu un nou act național general privind protecția, care ar elabora și completa GDPR. Cu toate acestea, proiectul de lege al Guvernului privind noua lege privind protecția datelor este încă în curs de revizuire de către Parlament și, prin urmare, noua lege privind protecția datelor nu a fost încă adoptată.

FRANȚA

Legea nr. 78-17 privind tehnologia informației, fișierele de date și libertățile civile din 6 ianuarie 1978 (DPA). Acest act a fost modificat pentru a pune în aplicare Directiva 95/46 / CE privind protecția datelor (Directiva privind protecția datelor).

Decretul nr. 2005-1309 din 20 octombrie 2005[18].

DPA a fost recent modificată substanțial prin Legea nr. 2016-1321 pentru o Republică digitală din 7 octombrie 2016 (Legea digitală a Republicii). În parte, amendamentul a fost făcut pentru a pregăti intrarea în vigoare a Regulamentului (UE) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date la 25 mai 2018.

Autoritatea franceză pentru protecția datelor (CNIL) supraveghează aplicarea DPA și emite frecvent decizii și linii directoare privind aceasta.

[17] http://eelnoud.valitsus.ee/main/mount/docList/1909e111-ca98-4d1b-830a-ee49dea64a97#R7f5TQiu
[18] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000241445

Există o serie de legi și reglementări privind protecția datelor cu caracter personal care reglementează sectoare specifice, printre care:

Codul comunicațiilor poștale și electronice[19] (art. L34 și art. R10) (reglementarea serviciilor publice de comunicații electronice online).

Codul de consum (L 223-1)[20] (privind telemarketingul).

Codul Consumatorului [21](L 224-42 până la L 224-42-4). Acestea au intrat în vigoare la 25 mai 2018 și stabilesc un principiu general conform căruia consumatorii au dreptul să recupereze toate datele lor.

Codul de sănătate publică[22] (articolele L 1110-4 și următoarele, L 1111-8 și următoarele, L 1115-1 și următoarele, L 1122-1 și următoarele, L 1435-6, L 1460-1 și următoarele, R 1111-1 et seq) (privind prelucrarea datelor privind sănătatea).

Codul proprietății (articolul L 212-3)[23] (privind reținerea datelor cu caracter personal conținute în arhivele publice).[24]

TAJ – Abordarea antecedentelor judiciare [25]

Prelucrarea antecedentelor judiciare (TAJ) este un dosar comun poliției și jandarmeriei naționale, înlocuind dosarele STIC ale poliției naționale și JUDEX, ale jandarmeriei naționale, care au fost șterse definitiv.

Abordarea antecedentelor judiciare (TAJ), în aplicarea articolelor 230-6-230-11 din Codul de procedură penală, este folosit în contextul investigațiilor judiciare (căutarea făptuitorilor infracțiunilor) și anchetelor administrative (cum ar fi anchetele înainte de anumite locuri de muncă publice sau sensibile).

[19] http://www.wipo.int/wipolex/en/details.jsp?id=14290

[20] https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069565&idArticle=LEGIARTI000032226761

[21] https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069565&idArticle=LEGIARTI000033206912&dateTexte=&categorieLien=id

[22] https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072665&idArticle=LEGIARTI000036515027&dateTexte=&categorieLien=id

[23] https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000006279036&dateTexte=&categorieLien=cid

[24] https://uk.practicallaw.thomsonreuters.com/6-502-1481?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1#co_anchor_a429186

[25] https://www.cnil.fr/fr/taj-traitement-dantecedents-judiciaires

Autorizațiile de procesare a datelor TaJ au fost emise:

- în scopul investigațiilor judiciare: ofițeri și membri ai poliției naționale și ai jandarmeriei care efectuează misiuni de poliție judiciară desemnate individual, vamele judiciare, procurorii, agenții serviciilor judiciare autorizați de procuror.
- pentru efectuarea anchetelor administrative: personalul de poliție și jandarmerie autorizat, agenții serviciilor de informații specializate menționați la articolul R. 234-2 din Codul de securitate internă, ofițerii Serviciului de Investigare a Securității Naționale (SNEAS) și Comandamentul Specializat pentru Securitate Nucleară (CoSSeN), personalul investit în misiuni administrative de poliție autorizate de reprezentantul statului.

Decretul nr. 2018-687 din 1 august 2018 prevede că persoanele au acum dreptul de a accesa și de a rectifica acest dosar direct de la Ministerul de Interne (articolul R.40-33 II din Codul de procedură penală).

Anonimizare şi minimizare

1. Decizie exemplu:

Formarea restrânsă a CNIL, după deliberare, decide: să pronunțe împotriva asociației ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE o sancțiune pecuniară în valoare de treizeci de mii (30.000) euro; pentru a-și publica deliberarea, care va fi anonimă la sfârșitul a doi ani de la publicarea sa.[26]

2. *Pentru a consulta starea dosarului dvs., trebuie să introduceți codul confidențial menționat în scrisorile trimise de către registru. Acest serviciu vă permite să consultați un rezumat al informațiilor referitoare la dosarul dvs. Acest serviciu este destinat utilizării exclusive a părților.*[27]

https://casier-judiciaire.justice.gouv.fr/pages/accueil.xhtml

GERMANIA

La 1 februarie 2017, cabinetul german a adoptat un proiect de lege pentru adaptarea legislației privind protecția datelor. Aceasta marchează începutul procesului legislativ de înlocuire a Legii federale privind protecția datelor, care datează din 1977. Legea pentru a transpunerea Regulamentului (UE) 2016/679 și pentru a implementa

[26] https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037435170&fastReqId=279071783&fastPos=1

[27] https://sagace.juradm.fr/Authentification.aspx

Directiva (UE) 2016/680 privind protecția datelor este cunoscută sub numele Bundesdatenschutzgesetz[28].

Legea privind confidențialitatea germană (Bundesdatenschutzgesetz - BDSG) prevede reguli și cerințe generale pentru prelucrarea datelor atât în sectorul public, cât și în sectorul privat. Legiuitorul german a folosit clauzele de deschidere și a redactat noul BDSG[29] pentru a adapta legea germană privind confidențialitatea la cerințele GDPR și Directiva UE privind confidențialitatea pentru poliție și justiție (Directiva UE 2016/680). Există riscul ca instanțele și autoritățile de supraveghere să nu aplice legea, deoarece consideră că aceasta este o încălcare a legislației europene.

Judecătorii germani nu sunt legați de un precedent (Präjudizien), ci, în vederea consecvenței, aceștia pot lua în considerare deciziile anterioare ale curții superioare. Judecătorii germani interpretează și aplică legea existentă doar în faptele pe care le au în fața lor.

Jurnalul de drept NJW-RR publică decizii de drept civil / comercial. Acesta este disponibil prin intermediul BeckOnline și tipărit în Legea Bod.[30]

Organizarea justiției în Germania[31]

Informații privind punerea în aplicare a dispozițiilor de protecție a datelor prevăzute la articolele 13-14 din Regulamentul general privind protecția datelor (GDPR)[32]

Deciziile Curții Federale de Justiție începând cu 1 ianuarie 2000 pot fi găsite online în baza de date. Deciziile sunt acordate gratuit numai pentru utilizare necomercială (§ 11 alin. 2 teză 2 JVKostG)

Curtea Federală de Justiție procesează datele personale în proceduri reglementate legal pentru a-și îndeplini atribuțiile. Datele personale sunt, de exemplu, informații personale și despre fapte care sunt legate de persoana vizată. În timpul procesării, se respectă cele mai înalte cerințe privind securitatea datelor.

Datele personale vor fi procesate numai dacă acest lucru este necesar pentru îndeplinirea atribuțiilor Curții Federale de Justiție sau dacă persoana vizată consimțit în mod expres (§ 3 BDSG).[33]

[28] https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf
[29] https://germanlawarchive.iuscomp.org/wp-content/uploads/2014/03/BDSG.pdf
[30] https://libguides.bodleian.ox.ac.uk/c.php?g=422919&p=2888159
[31] https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-de-en.do?member=1
32 http://www.bundesgerichtshof.de/DE/Oben/Datenschutz/datenschutz_node.html

[33] http://www.bundesgerichtshof.de/DE/Oben/Datenschutz/datenschutz_node.html

Baza juridică a operațiunilor de prelucrare a datelor legate de îndeplinirea atribuțiilor și competențelor organelor judiciare sunt articolul 6 alineatul (1) literele (c) și (e) și articolul 9 alineatul (2) litera (f) din GDPR și dispozițiile relevante ale regulamentul de procedură respectiv.

Chiar și după finalizarea unui proces, datele pot fi prelucrate pentru a îndeplini alte obligații legale, astfel încât să respecte cerințele de păstrare legală. Se aplică apoi dispozițiile Regulamentului general privind protecția datelor (GDPR) și Legii federale privind protecția datelor (BDSG).

Pentru prelucrarea datelor cu caracter personal în legătură cu prevenirea, investigarea, depistarea, urmărirea penală sau sancționarea infracțiunilor sau a infracțiunilor, se face trimitere la dispozițiile părții a 3-a capitolul 3 §§ 55-61 din Legea federală privind protecția datelor (BDSG).

Cui sunt datele dezvăluite?

a) receptor

În cadrul Curții Supreme Federale obțin acces la datele personale numai acele persoane cărora li se încredințează efectuarea procedurii în care datele sunt relevante pentru procedură. Acestea sunt în special judecătorii responsabili de procedura respectivă, precum și alți angajați ai instanței și reprezentanții acestora.

Datele vor fi divulgate terților doar pe baza unor reglementări legale, a altor baze juridice sau, în cazul în care consimțământul explicit este dat.

b) Categorii de destinatari

Curtea Federală de Justiție transmite date cu caracter personal în cazuri individuale.

Parte a procedurii în care au fost colectate datele personale, în măsura necesară desfășurării procedurii; în conformitate cu regulile de procedură respective care urmează să fie numite în procedură persoane, z.;

Experți sau interpreți. Martorii vor fi expuși la informațiile personale, după cum este necesar pentru a realiza un proces; alte instanțe, în măsura în care acestea sunt necesare pentru îndeplinirea sarcinilor lor;

Autorități, cum ar fi autoritățile de securitate, pentru sarcini statutare;

Alte persoane implicate în proceduri privind registrul Curții Federale de Justiție sau alte persoane care au dreptul de a depune o inspecție în conformitate cu regulamentul de procedură respectiv sau cu alte dispoziții legale.

Pe pagina Curții Federale de Justiție s-a folosit anonimizarea în sensul în care: deciziile Curții sunt publice, apar numele judecătorilor, procurorilor, avocaților, sunt

descrise întâmplările ori situațiile judecate însă, nu exista nume de inculpat, de reclamant. Anonimizarea se face prin numele de dosar care apare la început, astfel se asigura protectia datelor personale ale celor implicati in dosar.

Practici online

1. Tribunalul regional (Landgericht) Bonn (printr-o decizie din 29 mai 2018, cazul nr. 10 O 171/18 - numai în limba germană), prima instanță germană care a pronunțat o hotărâre cu privire la aplicarea practică a GDPR. Acest lucru face, probabil, decizia instanței de judecată prima decizie a instanței GDPR în întreaga lume, iar decizia s-a referit la problema hot-button de disponibilitate publică a ICANN "date WHOIS".[34]

Instanța a fost chemată să se pronunțe printr-o hotărâre provizorie privind principiul minimizării datelor prevăzut la art. 5 (1) lit. c) GDPR. Părțile la procedură au fost Corporația de Internet pentru numere și numere alocate (ICANN) împotriva registratorului acreditat de către ICANN, EPAG Domainservices GmbH, cu sediul în Germania. ICANN a căutat să oblige EPAG să respecte "Acordul de acreditare a registratorului" al ICANN, care impune registratorilor să colecteze informații de contact administrative (Admin-C) și tehnice (Tehnic-C) pentru o nouă înregistrare a numelor de nume de domeniu ("Date WHOIS"). Instanța a decis că ICANN nu ar putea să demonstreze în mod credibil că colecția de Admin-C și Tehnic-C este necesară în conformitate cu art. 5 (1) lit. c) GDPR și, prin urmare, EPAG nu este obligat să colecteze astfel de date.

2. Problemele tradiționale ale probelor pot fi, de asemenea, diminuate în cadrul GDPR. Articolul 82 GDPR este structurat astfel încât companiile sunt susceptibile de a fi răspunzătoare de îndată ce acestea sunt "implicate în" prelucrare, dar pot răsturna această prezumție demonstrând că nu sunt în niciun fel "responsabili" pentru prejudiciul reclamantului. Unii comentatori germani au sugerat că acest lucru introduce o răspundere fără vină pentru încălcarea confidențialității. Drept urmare, reclamanții germani ar trebui să demonstreze doar că o societate este "implicată în" prelucrare pentru a se recupera de la societate; atunci ar fi sarcina companiei de a arăta că nu poartă nici o vină pentru încălcarea drepturilor de confidențialitate. Având în vedere raționamentele privind protecția consumatorilor în ceea ce privește legislația privind protecția datelor, ar putea fi dificil pentru companii să susțină cu succes că nu sunt în nici un fel "responsabili" pentru daunele legate de viața privată.

Chiar și atunci când GDPR nu solicită în mod specific numirea unui DPO, organizațiile pot uneori să fie utile să desemneze unul pe bază de voluntariat. Grupul de lucru pentru protecția datelor în temeiul articolului 29 ("WP29") încurajează aceste

[34] https://blogs.dlapiper.com/privacymatters/germany-first-court-decision-on-gdpr/

eforturi voluntare. WP29 consideră că o astfel de noțiune trebuie stabilită în conformitate cu legislația națională.

ITALIA

Consiliul de Miniștri al Italiei a aprobat Decretul legislativ nr. 101/2018[35], care armonizează Codul italian de confidențialitate și alte legi naționale cu Regulamentul european general privind protecția datelor. Decretul intră în vigoare la 19 septembrie 2018 și abordează numeroase domenii esențiale, de la procesarea datelor anumitor categorii de date personale (sensibile, juridice, genetice și biometrice) la copii și drepturile persoanelor decedate, trecând prin coduri de conduită în conformitate cu Codul de confidențialitate și redefinirea dreptului penal pentru a sprijini îndeplinirea corectă a obligațiilor care decurg din această chestiune.

În 2016, parlamentarii europeni au decis să lase fiecărui stat membru un anumit spațiu de manevră. Din acest motiv, în cadrul GDPR există anumiți pași importanți lăsați în sarcina statelor membre. Scopul acestei proceduri este de a adapta legile diferitelor tipuri de societăți și de sisteme juridice, păstrând, de asemenea, particularitățile criticate de autoritățile naționale de protecție a datelor în decursul anilor.

Articolul 2 al legii italiene pare să introducă o referință importantă la lege și la regulamente ca temei juridic, precum și o asumare a legalității prelucrării "pentru îndeplinirea unei sarcini îndeplinite în interesul public sau în exercitarea funcției oficiale autoritate "și pentru comunicarea de date de la un subiect la altul în acest context.

Cu referire la articolele 15-22 din GDPR, drepturile persoanelor vizate vor fi limitate sau excluse în cazuri specifice atunci când acestea sunt în contradicție cu alte cerințe impuse de legislația națională, ca în cazul aplicării spălării banilor, urmărind prerogativele comisiilor parlamentare de anchetă, prelucrările efectuate pentru apărarea activităților de investigare sau exercitarea unui drept în instanță sau chiar în caz de avertizare. Aceleași drepturi, dacă sunt legate de persoane decedate și cu anumite limitări, pot fi exercitate de aceia care au un interes propriu sau care acționează pentru a proteja persoana în cauză sau "din motive familiale care merită protecție".

Sancțiunile penale deja introduse de Codul de confidențialitate au fost reorganizate și reformulate. Noile sancțiuni vor viza: prelucrarea ilegală a datelor; comunicarea ilegală și divulgarea datelor prelucrate la scară largă; neadevărul în comunicarea către Garante și întreruperea activităților DPA italiană; nerespectarea

35 http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=false

prevederilor din Garante; încălcări ale dispozițiilor privind controalele la distanță și sondajele privind opiniile lucrătorilor.

Tribunalul Milano - consultare publică[36]

Punctul de informare privind dezbaterile penale și hotărârile GIP [37]

Legea a fost publicata in septembrie 2018.[38] Aici monitorul oficial

LITUANIA

Parlamentul lituanian a adoptat noua lege[39] privind protecția juridică a datelor cu caracter personal din 30 iunie 2018. Legea adoptată a intrat în vigoare la 16 iulie. Inspectorul de Stat pentru Protecția Datelor și Oficiul Inspectorului pentru Etică Jurnalistică - ambele însărcinate cu supravegherea și aplicarea legii și GDPR în Lituania – au fost obligate să adopte ordonanțe de punere în aplicare până pe 15 iulie.

Legea, care constă în 35 de articole, este destul de concisă și vizează în principal particularizarea competențelor autorităților de supraveghere. Printre alte prevederi notabile se numără următoarele:

Aplicarea teritorială. Legea se aplică controlorilor și prelucrătorilor stabiliți în Lituania, precum și controlorilor care respectă legea lituaniană în virtutea dreptului internațional public. În ceea ce privește întreprinderile care oferă bunuri sau servicii sau monitorizarea comportamentului persoanelor vizate în UE, legea se aplică numai acelor controlori și prelucrătorilor care au desemnat un reprezentant în Lituania. Acest lucru pare să implice faptul că, de exemplu, o afacere asiatică care vizează persoanele în Lituania, fie poate desemna un reprezentant în Germania, fie este scutită de desemnarea unui reprezentant (articolul 27 alineatul (2) din GDPR) fie nu a desemnat reprezentant încălcând articolului 27 din GDPR, însă nu va avea obligația să respecte legea.

Prelucrarea în contextul ocupării forței de muncă. Legea prevede norme mai specifice în ceea ce privește prelucrarea datelor cu caracter personal în contextul ocupării forței de muncă. Aceste reguli trebuie citite împreună cu obligațiile angajatorului conform noului Cod al Muncii. Legea interzice în mod explicit prelucrarea datelor angajaților cu privire la condamnările și infracțiunile penale, cu excepția cazului

[36] https://www.tribunale.milano.it/index.phtml?Id_VMenu=482
[37] https://www.tribunale.milano.it/index.phtml
[38] http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true
[39] https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/952a77b0709011e8a76a9c274644efa9

în care o astfel de prelucrare este necesară pentru a determina caracterul adecvat al persoanei de a îndeplini cerințele pentru poziția în conformitate cu legile relevante.

Angajatorii pot colecta informații despre calificările sau calitățile profesionale ale viitorului angajat de la foștii angajatori numai după ce l-au informat pe candidat despre această procesare, în timp ce pentru a colecta aceleași informații de la angajatorul actual al persoanei, va trebui să obțină consimțământul prealabil al angajatului. De asemenea, angajatorii au o nouă obligație de a informa angajații, în conformitate cu articolul 13 din GDPR, cu privire la supravegherea video sau audio, urmărirea comportamentului, localizarea sau deplasarea.

Consimțământul digital al copilului. Lituania (împreună cu Bulgaria, Austria și Cipru) a optat pentru 14 ani ca vârstă de "consimțământ digital".

Atribuțiile autorităților de supraveghere

Competențele de supraveghere și executare sunt împărțite între Inspectoratul de Stat pentru Protecția Datelor (DPA) și Oficiul Inspectorului pentru Etică Jurnalistică. Competența acestora este limitată la supravegherea prelucrării datelor cu caracter personal în scopuri jurnalistice și a scopurilor exprimării academice, artistice sau literare. Atunci când își exercită atribuțiile, inspectorul pentru etică jurnalistică trebuie să colaboreze cu DPA pentru a asigura aplicarea consecventă a legilor privind protecția datelor.

Legea prevede în continuare competențe suplimentare ale DPA și precizează anumite proceduri care trebuie urmate de cele două autorități de supraveghere.

Certificare. Legea prevede o nouă putere a DPA de a acredita organismele de certificare. Aceste organisme, în conformitate cu articolul 43 din GDPR, vor emite certificarea în cadrul mecanismelor de certificare a protecției datelor. Regulile de acreditare vor fi elaborate de DPA.

Reprezentarea persoanelor vizate. Legea permite unui subiect să mandateze un organism, organizație sau asociație nonprofit să depună o plângere în fața autorităților de supraveghere în numele său. Această entitate va trebui să furnizeze documentația care să ateste că operează în domeniul protecției datelor. Legea nu indică ce documente trebuie furnizate, cel mai probabil, acest lucru va fi evaluat de la caz la caz. De asemenea, legea nu oferă organizațiilor de drepturi de confidențialitate dreptul de a depune o plângere independent de mandatul persoanei vizate (articolul 80 alineatul (2) din GDPR).

În mod evident, legea nu oferă toate răspunsurile pe care le-au căutat controlorii și procesatorii din Lituania. Multe întrebări importante, inclusiv operațiunile de prelucrare care necesită o autorizație obligatorie, o procedură pentru o consultare prealabilă cu DPA și cerințele pentru organismele de certificare, vor fi abordate în norme care urmează să fie adoptate de autoritățile de supraveghere.

MALTA

Regulamentul general privind protecția datelor (UE) (2016/679) GDPR a fost pus în aplicare prin Legea privind protecția datelor din Malta din 2018 (capitolul 586 din legile Maltei)[40] ("DPA"), care a intrat în vigoare la 28 mai 2018.

Datele personale sunt informații referitoare la o persoană fizică identificată sau identificabilă.

Acesta este un termen larg și include o gamă largă de informații. GDPR afirmă în mod expres că include identificatori online, cum ar fi adresele IP și identificatorii cookie-urilor.

Întreaga prelucrare a datelor cu caracter personal trebuie să respecte toate cele șase principii generale privind calitatea datelor. Datele cu caracter personal trebuie: (a) să fie procesate corect și legal; (b) colectate în scopuri specifice, explicite și legitime și nu sunt prelucrate într-o manieră incompatibilă cu aceste scopuri; (c) adecvate, relevante și nu excesive; (d) exacte și, dacă este necesar, actualizate; (e) să fie păstrate într-o formă care să nu poată fi identificată mai mult decât este necesar; și (f) păstrată în siguranță.

Prelucrarea datelor cu caracter personal trebuie să îndeplinească, de asemenea, cel puțin o condiție pentru prelucrarea datelor cu caracter personal. Aceste condiții constau în faptul că prelucrarea este: (a) efectuată cu consimțământul persoanei vizate; (b) necesare pentru executarea unui contract cu persoana vizată; (c) necesare pentru respectarea unei obligații legale; (d) este necesar pentru a proteja interesele vitale ale persoanei vizate; (e) necesare pentru interesul public sau în exercitarea autorității publice; sau (f) necesare pentru interesele legitime ale operatorului sau ale destinatarului, cu excepția cazurilor în care sunt suprascrise de interesele persoanei vizate.

Prezentul act nu se aplică prelucrării datelor cu caracter personal:

(a) în cursul unei activități care nu intră sub incidența dreptului Uniunii;

(b) de către guvernul Maltei atunci când desfășoară activități care intră sub incidența titlului V capitolul 2 din Tratatul privind Uniunea Europeană;

(c) de către o persoană fizică în cursul unei activități pur personale sau gospodărești; sau

(d) de către autoritățile competente în scopul prevenirii, cercetării, depistării sau urmăririi penale a infracțiunilor sau executării de sancțiuni penale, inclusiv protejarea și prevenirea amenințărilor la adresa securității publice, după consultarea cu comisarul

[40] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12839&l=1

și cu acordul ministrului responsabil cu poliția, ministrul să poată prevedea dispoziții privind prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, cercetării, depistării sau urmăririi penale a criminalității infracțiunile sau executarea sancțiunilor penale, inclusiv protecția împotriva și prevenirea amenințărilor la adresa securității publice.

OLANDA

La 22 mai 2018, Legea privind implementarea GDPR[41] a fost publicată în Jurnalul Oficial al Regatului Țărilor de Jos, finalizând procesul legislativ care a început oficial la 12 decembrie 2017. În Decretul Regal care îl însoțește, Ministrul pentru Protecția juridică a anunțat că legea se va aplica începând cu data de 25 mai 2018, aceeași dată în care GDPR ar intra în vigoare.

Secțiunea 3.2 Datele cu caracter personal de natură penală, și în special articolele 32 – 42 menționează despre excepții și recomandări privind datele cu caracter personal .

Articolul 32. Motive generale de exceptare privind informațiile de natură penală. Datele personale de natură penală pot fi prelucrate dacă:

a. persoana vizată a dat în mod explicit permisiunea de a prelucra aceste date cu caracter personal în unul sau mai multe scopuri specifice;

b. prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale altei persoane fizice, în cazul în care persoana vizată nu este capabilă din punct de vedere fizic sau legal să-și dea consimțământul;

c. prelucrarea se referă la datele cu caracter personal care au fost făcute publice de persoana vizată;

d. procesarea este necesară pentru instituție, exercitarea sau fundamentarea unei cereri legale sau atunci când instanțele acționează în contextul capacității lor juridice;

e. prelucrarea este necesară din motive de interes public superior, astfel cum se menționează la articolul 23 literele (a) și (b); sau

f. prelucrarea este necesară în scopul cercetării științifice sau istorice sau în scopuri statistice în conformitate cu articolul 89 primul paragraf din regulament și sunt îndeplinite condițiile menționate la articolul 24 literele (b) și (d).

[41] https://zoek.officielebekendmakingen.nl/stb-2018-144.html

Articolul 35. Aplicarea dreptului civil prin decizia organelor neadministrative

(1) În cazul în care decizia privind o cerere menționată la articolul 34 a fost luată de un alt organism decât o autoritate administrativă, partea interesată poate înainta instanței, cu solicitarea scrisă, obligarea operatorului de a solicita cererea menționată la articolele 15-22 din regulament sau să o respingă.

2. Petiția se depune în termen de șase săptămâni de la primirea răspunsului din partea operatorului. În cazul în care operatorul nu răspunde în termenele prevăzute la articolul 12 alineatul (3) din regulament, prezentarea petiției nu face obiectul unei limite de timp.

3. Curtea districtuală va acorda cererea în măsura în care consideră că aceasta este întemeiată. Înainte ca instanța să decidă, va oferi, dacă este necesar, părților interesate posibilitatea de a-și prezenta opiniile.

4. Depunerea cererii nu trebuie făcută de un avocat.

5. A treia secțiune a celui de-al cincilea titlu al celei de-a doua cărți a Codului de procedură civilă se aplică mutatis mutandis.

6. Instanța poate solicita părților și altor persoane să furnizeze informații scrise și să prezinte documentele deținute de acestea într-un termen stabilit de instanță. Operatorul și partea interesată sunt obligate să respecte această solicitare. Articolele 8:45 al doilea și al treilea paragraf și 8:29 din Legea administrativă generală se aplică mutatis mutandis.

PORTUGALIA

În timp ce proiectul de lege care va pune în aplicare și aproba derogările de la Regulamentul general privind protecția datelor (GDPR) este încă în Parlament pentru a fi discutat și aprobat, Autoritatea portugheză pentru protecția datelor (CNPD) a publicat pe 25 mai o declarație împreună cu o listă din noile întrebări frecvente (FAQs), precum și formularele de raportare a numirii responsabilului cu protecția datelor (DPO) și a încălcărilor datelor.

CNPD a precizat că, deși adoptarea legislației naționale de punere în aplicare a GDPR în Portugalia, legea portugheză actuală privind protecția datelor (Legea 67/1998 din 26 octombrie[42]) va rămâne în vigoare în măsura în care nu contravine GDPR. În ceea ce privește prelucrarea datelor cu caracter personal referitoare la prevenirea, cercetarea și urmărirea penală, legea portugheză privind protecția datelor va rămâne pe deplin aplicabilă până în momentul în care în Portugalia va fi pusă în

[42] http://www.wipo.int/wipolex/en/details.jsp?id=3537

aplicare Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016. Prin urmare, CNPD își păstrează competențele conferite de Legea 67/98 în ceea ce privește prelucrarea datelor cu caracter personal referitoare la prevenirea, cercetarea și urmărirea penală și, în ceea ce privește prelucrarea datelor cu caracter personal acoperite de GDPR, CNPD procedează potrivit sarcinile și competențele conferite de noul regulament.

CNPD a anunțat, de asemenea, că va furniza un model pentru înregistrarea activităților de procesare, vizând în principal întreprinderile mici și mijlocii.

În ceea ce privește orientările CNPD emise până în prezent, acestea vor rămâne în vigoare și vor aplica, mutatis mutandis, fără a aduce atingere faptului că sunt actualizate în viitorul apropiat pentru a fi în conformitate cu GDPR.

În cele din urmă, CNPD evidențiază faptul că sancțiunile al GDPR sunt direct aplicabile.

SLOVACIA

Parlamentul slovac a publicat noua lege privind protecția datelor cu caracter personal (PDPA) în ianuarie 2018 sub numărul oficial 18/2018 cu intrare în vigoare la 25 mai 2018. (act no. 18/2018 coll. Slovakia[43])

PDPA este împărțită în șase părți. Partea a II-a reproduce majoritatea prevederilor GDPR și ar trebui să se aplice activităților de prelucrare care nu intră sub incidența legislației Uniunii Europene. Partea a III-a implementează prevederile Directivei privind aplicarea legii. Partea a IV-a prevede derogări și excepții locale față de GDPR. Părțile V și VI reglementează competența, sarcinile și competențele autorității slovene de supraveghere și alte dispoziții diverse.

Legiuitorul nu a reușit să profite de derogările permise de GDPR și există o serie de probleme cu PDPA, inclusiv punerea în aplicare a directivei privind aplicarea a Directivei (UE) 2016/680 – protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile polițienești și judiciare din sectorul penal și privind libera circulație a acestor date.

SPANIA

Spania este o țară în care cultura în materie de protecție a datelor este puternic înrădăcinată datorită normelor sale publicate încă din 1992. Legea organică 5/1992

43 https://www.konecna-zacha.com/en/new-slovak-data-protection-act-exceptions-to-the-gdpr/

din 29 octombrie privind Tratamentul automatizat al datelor (LORTAD), Legea organică 15/1999 din 13 decembrie privind protecția datelor (LOPD), Decretul regal 994/1999, din 11 iunie, care a aprobat Regulamentul privind măsurile de securitate pentru fișierele automatizate ce conțin date cu caracter personal (RSM) și Regulamentul de dezvoltare, Decretul regal 1720/2007, din 21 decembrie, care a aprobat Regulamentul de punere în aplicare a LOPD (RLOPD). Acest întreg compendiu legislativ constituie un cadru consolidat care dezvoltă articolul 18 alineatul (4) din Constituția spaniolă din 1978 (CE), care prevede că "legea va limita utilizarea procesării datelor pentru a garanta onoarea și intimitatea la viața privată și de familie a cetățenilor și exercitarea deplină a drepturilor lor". Aceste norme au consolidat bazele unui cadru juridic instituțional eficient și eficient pentru protecția datelor cu caracter personal în Spania. Noul GDPR reprezintă o provocare semnificativă pentru Spania, care a început în februarie 2018 prima discuție a proiectului în fața Parlamentului, cu patru luni înainte de aplicarea noului GDPR.

Ghid anonimizare spaniol [44]

Agentia nationala protectia datelor[45]

Site-ul curtii supreme:[46]

Înregistrare electronică. Selectați opțiunea pe care doriți să o faceți. Intrare în registru. Administrați noi înregistrări electronice de aici. Este necesar un certificat digital emis de o autoritate de certificare înregistrată.

SUEDIA

Comisia de anchetă guvernamentală suedeză, Comisia pentru protecția datelor, a publicat raportul său de anchetă (SwNy dataskyddslag SOU 2017: 39) privind abaterile naționale care sunt permise în conformitate cu Regulamentul general privind protecția datelor ("GDPR"), precum și impactul GDPR asupra legislației naționale.

Legea suedeză privind protecția datelor (2018: 218) și Regulamentul suedez pentru protecția datelor (2018: 219[47]), care conțin dispoziții suplimentare privind GDPR, au intrat în vigoare la 25 mai 2018.

[44] https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf
[45] https://www.aepd.es/normativa/index.html
[46] http://www.poderjudicial.es/cgpj/es/Poder_Judicial/Tribunal_Supremo
[47] http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2018219-med-kompletterande_sfs-2018-219