Treball Fi de Màster

Estudi del GDPR

Procediments i aplicació sobre asseguradores

Estudiant: Enric Belver Gonzalez

Tutors: Joan Josep Cabre Vicens / Josep Cañabate Pérez

Màster en Seguretat de les Tecnologies de la Informació i de les Comunicacions

UOC

Data: 31 de Maig de 2019

Abstract (Catala)

Des de mitjans de 2018 a la unió europea va entrar en vigor la nova normativa GDPR que introduïa noves regulacions en termes de protecció de dades i privacitat la qual va ser consumada després d'un període de negociacions des de 2016. Amb la introducció d'aquesta norma a tot el àmbit europeu les empreses han tingut que adaptar-se per poder complir-la creant nous procediments i mètodes per complir els seus diversos punts com poden ser el de Privacy by Design o el dret al oblit.

Passat un any de la implantació de la norma la situació general es una entre el compliment i la aproximació a la norma, moltes empreses s'han trobat que realitzar els canvis necessaris per complir les normes requereixen d'una inversió de recursos més gran de la esperada fent que les de petit o mitja mida amb recursos més limitats hagin tingut que prendre mesures per no tenir que enfrontares a sancions pel seu incompliment.

El TFM que es fa sobre la norma es divideix en dos parts, una part esta dedicada a analitzar i detallar el contingut de la norma en forma explicativa perquè qualsevol lector pugui entendre-la i ser capaç de visualitzar el context de la situació actual.

En una segona part es desenvoluparà una sèrie de procediments que una empresa de assegurances hauria de tenir per poder dir que compleix els requeriments proactius de la norma que requereixen que una empresa tingui una sèrie de mesures per cada un dels seus punts. La raó per la qual ens centrarem en una empresa de assegurances es per acotar el projecte i per proximitat del estudiant.

Abstract(English)

From the middle of 2018 to the European Union came into force the new GDPR regulations that introduced new regulations in terms of data protection and privacy which was completed after a period of negotiations since 2016. With the introduction of new regulations, This norm throughout the European area, companies have had to adapt to comply with new procedures and methods to fulfill their various points, such as Privacy by Design or the right to oblivion.

After one year of the implementation of the norm the general situation is one between compliance and approximation to the norm, many companies have found that making the necessary changes to meet the regulations require a larger resource investment of the It was hoped that those of small or medium size with more limited resources had to take measures to avoid having to face penalties for non-compliance.

The TFM that is done on the standard is divided into two parts, a part is devoted to analyze and detail the content of the norm in explanation so that any reader can understand it and be able to visualize the context of the current situation.

A second part will develop a series of procedures that an insurance company should have to be able to say that it meets the proactive requirements of the standard that require a company to have a series of measures for each of its points. The reason why we will focus on an insurance company is to reduce the project and the student's proximity.

Continguts

Introducció

Objectius

Els objectius principals d'aquest projecte es poden resumir en dos punts generals:

Anàlisis i resum del GDPR en un àmbit no tècnic/legal. La intenció es de fer un estudi sobre la norma des de la seva aparició fins al moment actual i esbossar-ne els detalls que la defineixen en un format comprensiu y que aclareixin la situació en que es troba y com progressarà en el temps la seva aplicació y ampliació amb noves mesures que s'estan desenvolupant.

Creació y desenvolupament de procediments per el compliment de la GDPR per a una empresa d'assegurances. Basant-nos ens els procediments retroactius que s'han tingut que crear en una empresa pel compliment de la norma es definirà una sèrie de nous procediments específics per una empresa d'aquestes característiques.

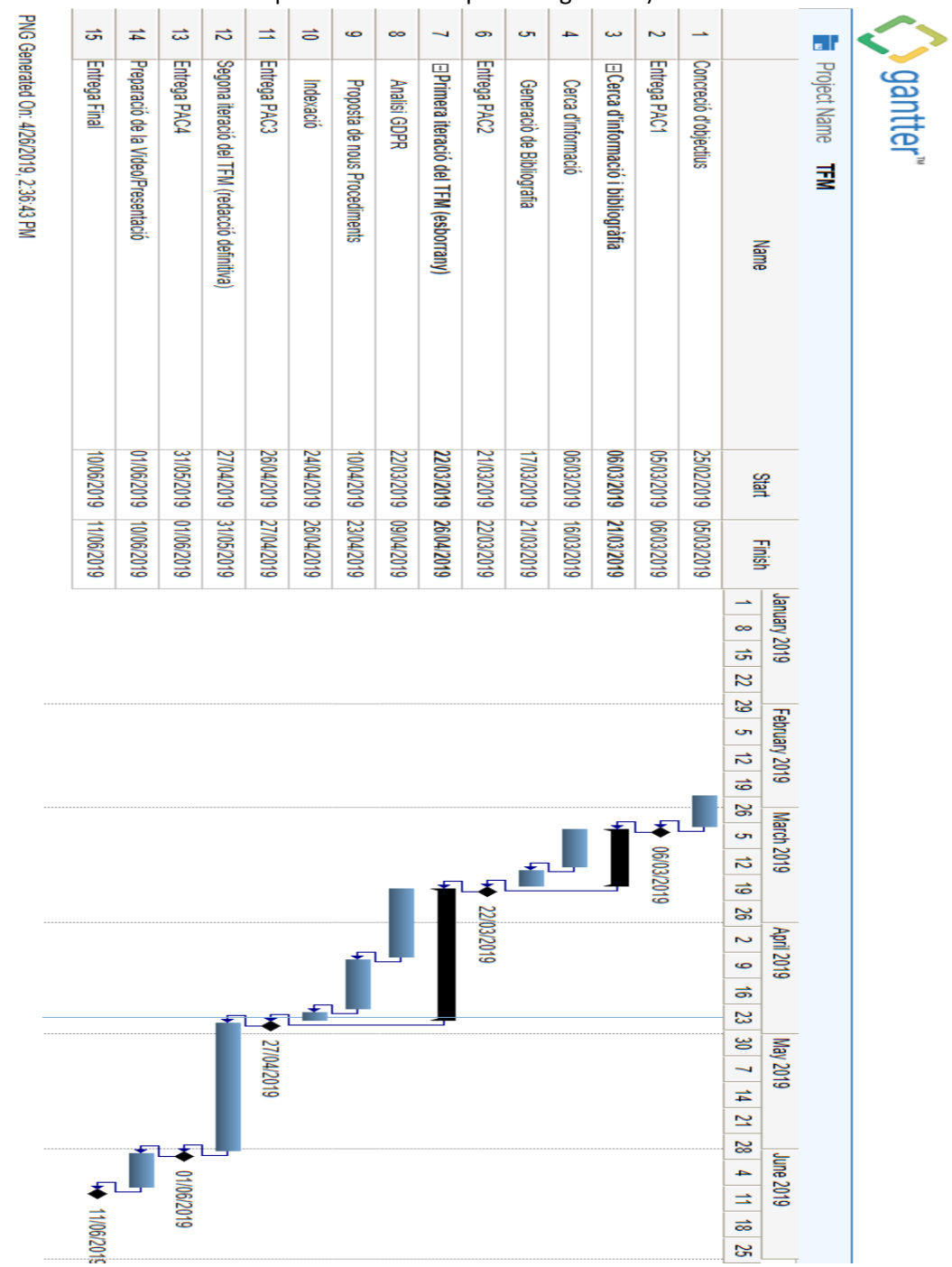
Metodologia

La metodologia que s'ha seguit per quest projecte ha sigut una primera part d'investigació on s'han recopilat fonts d'estudi i articles sobre el subjecte en qüestió per ampliar el coneixements del autor i poder començar a desenvolupar la primera part del TFM. Una vegada obtinguda la base necessària es va començar un treball d'investigació diferent, analitzant els procediments existents que s'han generat per la norma i comprendre el seu origen i necessitat.

Una vegada arribat a aquest punt es comença un treball de creació i desenvolupament de documentació on es junta el coneixement obtingut per les investigacions prèvies en genera documentació rellevant en la creació de procediments dirigits a assegurar el compliment de la norma per a una empresa de assegurances de forma que una empresa que tingui aquest procediments implantats compleixi totes les responsabilitats proactives que genera la norma.

Planificació

La planificació s'ha plantejant com un diagrama de gantt basant-se en les diverses entregues. (Per la redacció final intentarem posar una versió que es vegi millor)



GDPR

Que es?

El GDPR es una norma que crea un conjunt d'estàndards a tota la UE per a la protecció de dades personals digitals relacionades amb el comportament en línia o real dels usuaris d'Internet de la UE. És important destacar que aquestes normes s'apliquen a les dades personals dels usuaris d'internet de la UE, independentment de la ubicació de l'entitat que tingui les seves dades. En aquest sentit, les normes tenen un abast significatiu extraterritorial. Aquesta regulació substitueix la antiga directiva sobre política de dades, que havia establert un objectiu per a tots els països de la UE i pel seu compliments els estats membres individuals havien promulgar per separat una legislació nacional que aplicava els objectius de la directiva. El GDPR esta destinat a harmonitzar aquestes normes, però permet als estats membres individuals una discreció sobre una sèrie de disposicions. En el processament de dades, per exemple, hi ha flexibilitat en quines de les entitats que poden demostrar el compliment de GDPR, la transferència de dades fora de la UE i la llibertat d'expressió als mitjans de comunicació.

El GDPR defineix les dades personals com a "informació relativa a una persona física identificada o identificable". Aquesta comprensió de les dades personals inclou l'adreça IP, la identificació del dispositiu i el número de referència del client. És important destacar que aquestes proteccions s'apliquen a totes les entitats corporatives que processin les dades personals dels ciutadans de la UE, fins i tot si el tractament de dades rellevants no té lloc a la UE. La nova regulació també imposa restriccions a la transferència de dades personals fora de la UE. Les dades personals poden ser transferides fora de la UE només si la Comissió Europea determina que la jurisdicció receptora "assegura un nivell de protecció adequat" de manera coherent amb el GDPR; l'entitat processadora ha proporcionat "garanties adequades"; o l'individu ha proporcionat el consentiment específic per a la transferència. A més, el GDPR garanteix una sèrie de drets de privadesa per als usuaris d'internet de la UE, incloent-hi la notificació obligatòria i ràpida d'infraccions de dades que poden "comportar un risc per als drets i llibertats de les persones", accés a les dades personals, capacitat per instruir entitat per esborrar les dades personals i la capacitat de moure les dades personals d'una entitat de processament a una altra. Junts, aquests drets són el centre del propòsit de la regulació: "donar als ciutadans el control sobre les seves dades personals".

Aquests objectius es desenvolupen a través de diversos mecanismes. En primer lloc, les organitzacions que vulnerin les seves obligacions es poden multar fins a un 4 per cent de la seva facturació global anual o de 20 milions d'euros (el que sigui més gran). Aquesta multa s'aplica principalment a incompliments dels requisits de consentiment de GDPR, que estan relacionats amb el segon punt: Sota el GDPR, el consentiment ha de ser sempre inequívoc. Per a categories especials de dades personals (per exemple, raça o ètnia, opinió política, dades genètiques, afiliació sindical) es requereix un consentiment explícit. En tercer lloc, el GDPR exigeix que les entitats que controlin els titulars de les dades "a gran escala" o, de nou, que

processin categories especials de dades personals designin un agent de protecció de dades. Aquests oficials informen la seva organització sobre el compliment de GDPR, serveixen de punt de contacte per als titulars que informin de les seves dades i enllacen amb les autoritats supervisores de la UE. En quart lloc, el GDPR fomenta la creació de mecanismes de certificació de protecció de dades, de manera que les entitats poden demostrar clarament el compliment de la normativa. Els estats membres de la UE, així com les entitats de la Comissió Europea, tenen la facultat d'aplicar les disposicions.

Historic

22-06-2011

El Supervisor Europeu de Protecció de Dades publica un dictamen sobre la Comunicació de la Comissió Europea.

25-01-2012

La Comissió Europea proposa una reforma integral de les normes de protecció de dades de la UE per al 1995 per reforçar els drets de privadesa en línia i impulsar l'economia digital europea.

07-03-2012

El Supervisor Europeu de Protecció de Dades adopta un dictamen sobre el paquet de reforma de la protecció de dades de la Comissió.

12-03-2014

El Parlament Europeu demostra un fort suport al GDPR votant en ple, amb 621 vots a favor, 10 en contra i 22 abstencions.

27-07-2015

El Supervisor Europeu de Protecció de Dades publica les seves recomanacions als colegisladors europeus que negocien el text final del GDPR en forma de suggeriments de redacció. També llança una aplicació mòbil que compara la proposta de la Comissió amb els darrers textos del Parlament i del Consell

15-12-2015

El Parlament Europeu, el Consell i la Comissió arriben a un acord sobre el GDPR.

24-05-2016

El Reglament entra en vigor, 20 dies després de la publicació al Diari Oficial de la UE

06-05-2018

La directiva sobre protecció de dades per als sectors de la policia i la justícia a la legislació nacional aplicable a partir d'aquest dia

25-05-2018

El Reglament general de protecció de dades s'aplicarà a partir d'aquest dia en complet

Punts claus

El GDPR defineix les dades personals com qualsevol informació relacionada amb una persona física (persona interessada o titular de les dades) que es pugui utilitzar per identificar directa o indirectament a aquesta persona. Pot ser qualsevol cosa, des d'un nom, una foto, una adreça de correu electrònic, dades bancàries, publicacions a llocs web de xarxes socials, informació mèdica o fins i tot una adreça IP d'ordinador.

Sota una definició tan àmplia, les empreses han de prendre passos documentats per limitar l'accés a totes les dades personals només als empleats autoritzats i acreditats amb funcions que requereixen específicament l'accés a aquestes dades. Els incompliments de seguretat derivats de la falta d'aplicació dels protocols de seguretat es compliran amb multes i sancions financeres dures en el marc del GDPR.

El GDPR també estableix drets específics respecte a les persones interessades. Per complir amb el GDPR, aquests drets codificats han de ser reconeguts i implementats per totes les empreses que recullen dades personals sobre ciutadans de la UE.

Consentiment

El GDPR prohibeix específicament l'ús de termes llargs, complicats i declaracions de condicions, especialment en declaracions que contenen legals. Qualsevol sol·licitud de consentiment, declaració de termes o declaració de privadesa ha de ser presentada de manera clara i concisa i sense cap tipus d'ambigüitat de significat. A més, ha de ser tan fàcil retirar el consentiment com per donar-lo.

També fa clar que les empreses i organitzacions que gestionen dades privades o sensibles han de demanar consentiment i permís cada vegada que accedeixen a les dades. Segons la normativa, les empreses no poden demanar permís per accedir a dades privades una vegada i després considerar aquest accés per cobrir totes les transaccions futures. Segons el GDPR, no existeix un consentiment generalitzat; cada vegada que s'utilitzin dades per a un nou propòsit es requereix una nova sol·licitud de consentiment.

Notificació d'incompliment

El compliment del GDPR requereix que les empreses notifiquin a tots els interessats que s'ha produït un incompliment de seguretat dins de les 72 hores següents a la seva primera descoberta. El mètode d'aquesta notificació inclourà tantes formes com es consideri necessari per difondre la informació de manera oportuna, inclòs el correu electrònic, el missatge telefònic i l'anunci públic.

Dret d'accés

El GDPR exigeix a les empreses que facilitin, a petició de l'interessat, la confirmació de si s'està processant dades personals que pertanyen a elles, on s'està processant i amb quina finalitat. Les empreses també han de ser capaços de proporcionar, de forma gratuïta, una còpia de les dades personals que es processin en format electrònic.

Dret a ser oblidat

D'acord amb el GDPR, les empreses esborraran totes les dades personals quan l'interessat li ho sol·liciti. En aquest moment, la companyia cessarà la seva difusió i aturarà tot el processament. Les condicions vàlides per esborrar inclouen situacions en què les dades ja no són rellevants, o bé s'ha satisfet la finalitat original, o simplement la retirada posterior del consentiment d'un titular.

Portabilitat de dades

El GDPR exigeix a les empreses que proporcionin mecanismes perquè una persona interessada rebi qualsevol dada personal prèviament proporcionada en un format comunament utilitzat i llegible per màquina. Segons aquesta disposició, la persona interessada també té dret a sol·licitar a la companyia que transmeti les dades a un altre processador, de forma gratuïta.

Privadesa per disseny

Les empreses que compleixin els requisits han de seguir els principis de Privacitat per dissenyar i implementar mesures tècniques i organitzatives adequades de manera eficaç per satisfer els requisits del GDPR i protegir els drets dels interessats. En termes pràctics, aquesta disposició significa que les empreses processaran només les dades absolutament necessàries per a la realització del seu negoci i limitaran l'accés a les dades personals només als empleats que necessitin informació per completar el procés que l'autor atorga.

Oficials de protecció de dades

Les grans empreses que vulguin complir el GDPR mantindran registres exhaustius i exhaustius relacionats amb la recopilació, el processament i l'emmagatzematge de dades personals. A més, aquestes empreses designaran un responsable de protecció de dades (DPO en angles) per supervisar l'aplicació del GDPR i protegir les dades personals d'un mal ús i accés no autoritzat i altres infraccions de seguretat. Si una empresa compleix els criteris, un DPO designat és un requisit, no una opció.

Per desgràcia, per a les empreses de tot el món, els criteris específics per a quan una empresa està obligada a designar un DPO encara està en flux. Una regla general a seguir, basada en els escrits de la Comissió Europea sobre el tema, és que un DPO és necessari per a qualsevol empresa amb més de 250 empleats o per a qualsevol empresa que processi les dades personals de més de 5.000 interessats en qualsevol període de 12 mesos .

Implicacions

Les implicacions positives del GDPR

Seguretat cibernètica millorada

Les organitzacions han estat en una batalla contínua durant gairebé tot el temps que existeix Internet. Les actualitzacions de seguretat en xarxes, servidors i infraestructures han estat una font primordial de protecció cibernètica, juntament amb altres canvis de política i seguretat fins fa poc. L'aprovació de GDPR ha afectat directament els estàndards de privadesa i seguretat de les dades, alhora que incentiva indirectament les organitzacions a desenvolupar i millorar les seves mesures de seguretat cibernètica, limitant els riscos de qualsevol possible violació de dades.

Estandardització de la protecció de dades

Com es va esmentar al segon paràgraf, el compliment de GDPR és avaluat per les agències de protecció de dades de cada nació. Tot i que aquestes auditories de compliment són dutes a terme per agències independents, l'estandardització de l'entorn regulador a escala comunitària garanteix que una organització compleix GDPR i que poden operar de manera gratuïta a tots els països europeus sense haver de tractar amb la legislació de protecció de dades de cada país.

Seguretat de la marca

Com han experimentat algunes organitzacions reconegudes internacionalment, les infraccions de dades tenen un impacte monumental devastador en la reputació d'una organització. Els usuaris i els clients valoren la seva privadesa i la seva confiança es pot danyar irrevocablement si es produeix una infracció de dades i que la seva informació estigui disponible sense saber-ho. A l'extrem oposat d'aquest espectre, hi ha un client que està més que disposat a compartir la seva informació privada, ja que considera que les seves dades s'emmagatzemen i s'utilitzen d'acord amb GDPR. Si una organització pot convertir-se en un titular d'informació de confiança, les seves probabilitats de crear una relació duradora i fidel amb un client milloraran significativament.

Fidelització

Una de les raons principals per a la formació de GDPR era permetre que els usuaris passessin més temps en els llocs que gaudissin sense quedar-se descabellats amb anuncis de remitents no sol·licitats o d'organitzacions relativament desconegudes que estaven subscrits en el passat. Els usuaris i els clients són molt més susceptibles d'acceptar l'acceptació obligatòria d'organitzacions i empreses que els interessen. En un futur pròxim, un usuari que subscrigui a una organització serà el que qualifiqui el seu interès en les subscripcions convertint-se en un signe de fidelització. o interessos.

Les implicacions negatives del GDPR

Sancions per incompliment

El cost de l'incompliment és sens dubte el que ha animat a les organitzacions a considerar les seves responsabilitats en matèria de protecció de dades dins de la UE. Amb una multa potencial de 20 milions d'euros o el 4% de la xifra de negocis anuals globals, el cost d'incompliment, els resultats d'una auditoria poden suposar una realització aterridora del tancament de les empreses si una organització no protegeix les dades dels seus clients.

El cost dels canvis per la conformitat de la norma

Quan va sorgir la primera notícia de la implementació de la GDPR el 2018, la majoria de les organitzacions van reaccionar instar un responsable de protecció de dades per assumir la responsabilitat de garantir que les polítiques internes estiguessin actualitzades i que s'implementessin els processos necessaris. Depenent de la quantitat de dades de ciutadans de la UE que siguin processats per una organització, el cost d'aconseguir el compliment pot variar de centenars d'euros a desenes de milers. Tot i que GDPR té certes implicacions molt positives tant per a les empreses com per als usuaris, el cost d'aquest tipus pot acumular-se amb força rapidesa i afegir-hi salaris imprevistos.

Sobreregulació

La nova legislació també va acompanyada de la possibilitat de sobreregulació. L'addició d'una doble opció dins d'un formulari presenta al client modern un missatge de consentiment inacabable. El nou formulari de consentiment permet als clients controlar si i com es posa en contacte per una organització, donant-los el control total de qui i com comparteixen les seves dades. La presència contínua d'aquesta activitat pot desincentivar alguns clients a registrar-se, ja que retarden l'exigència d'incorporar-se fins que estiguin totalment segurs del seu interès.

Futur – Noves regulacions e Incidències

ePrivacy

El Reglament de ePrivacy electrònica substituirà la Directiva de privadesa i comunicacions electròniques de 2002. El fet que sigui una regulació és important, ja que això significa que serà un acte legal i serà executable immediatament en tots els àmbits dels estats membres de la UE, a diferència d'una directiva, que permet als estats introduir els seus propis mecanismes, sempre que coincideixin amb l'esperit de la directiva original.

Mentre que el GDPR es centra a protegir les dades personals, la normativa de privadesa electrònica consisteix més a protegir la privadesa personal (tant per a les persones com per a les empreses) a través de les comunicacions electròniques. La distinció és important, com veuràs quan parlem de l'abast del reglament de privadesa electrònica i dels tipus de serveis als quals s'aplica.

Significativament, el Reglament de ePrivacy electrònica tracta temes específics, que estableixen normes específiques al voltant d'aquests temes, dins l'abast de GDPR. Quan es posi en pràctica el Reglament de privadesa electrònica, GDPR se situarà per sobre d'ella i continuarà aplicant-se a àrees de protecció de dades més àmplies que el Reglament de privadesa electrònica no cobreix.

El Reglament inclou una disposició que permet als estats membres mantenir o introduir disposicions nacionals addicionals per ajudar en la implementació i la interpretació en el context de les lleis existents. En altres paraules, l'abast total de la regulació original serà el mateix entre els estats membres, però la seva aplicació pot variar.

Article 13

L'article 13 de la Directiva de propietat intel·lectual de la Unió Europea al mercat únic digital amplia la responsabilitat legal de les empreses tecnològiques, de manera que s'hauran de filtrar automàticament el material protegit amb drets d'autor que s'ha carregat a les seves plataformes, llevat que s'hagi concedit una llicència específica. Això ha convertit en una controvertida llei de propietat intel·lectual.

Els crítics de l'article 13 han manifestat la seva preocupació sobre la censura d'Internet que podria sorgir de la nova directiva, concretament que els *memes* poguessin ser prohibits. Algunes de les principals companyies tecnològiques han expressat qüestions com el cost de filtrar contingut. Mentrestant, algunes discogràfiques, artistes i companyies de mitjans de comunicació donen suport a les reformes de la protecció dels drets d'autor per assegurar-se que es paguen amb justícia pels continguts produïts.

Procediments

En aquesta secció s'introduirà la llista de procediments generats per a una empresa d'assegurances (no exhaustiu)p er complir les responsabilitat que atribueix a la empresa la normativa GDPR. Per facilitar-ne la lectura i seguiment aquest estaran separats per categories i subcategories depenent de el seu objectiu i "zona" d'aplicació

Procediments de govern

Responsabilitat i compliments

Degut al tipus d'informació que gestiona una empresa d'assegurances aquesta ha de estar subjecte a avaluacions i auditories freqüents sobre com es gestionen aquestes dades i com els impacte el processament al que estan sotmeses.

Per complir la normativa GDPR una empresa d'assegurances ha de implementar un mínim de mesures tècniques i organitzatives per garantir la protecció d'aquestes a mes de demostrar a traves de documentació i practica el seu compliment

La empresa operarà amb "Privacy by design" com a ètica central en el seu tractament de dades aplicant una sèrie de mesures i processos en el seu tractament per mitigar qualsevol risc associat amb aquesta. Entre el processos que es seguiran incloem la minimització de dades al més basic o necessari. Seguint el principis definits per la normativa GDPR nomes es recol·lectarà, guardarà, compartirà i processarà les dades essencial per poder dur a terme els serveis de la empresa o requisit legals.

Tant els treballadors com els sistemes de la empresa nomes sol·licitaran per disseny las dades rellevant per a dur a terme el procés. Amb aquest sistema es reduiran els riscos de fuga de dades, el que recíprocament ajudarà al compliment de la normativa. Algunes de les mesures presses influeixen:

- Formularis estandarditzats per els processos electrònics que nomes inclouen camps per les dades rellevant excloent cap element que es pogués considerar opcional.

- Formularis físics estandarditzats per a qualsevol procés manual de recol·lecció de dades, aquest també excloent cap dada que es pugui considera opcional.

- Sistemes de filtratge en recepció de dades de tercer que asseguren que nomes les dades requerides son rebudes i guardades excloent qualsevol dada opcional o innecessària

- Tot formulari i element de recol·lecció de dades tant en àmbit físic o digital es revisat quadrimestral ment per assegurar que compleix les normatives i es efectiu a la hora de sol·licitar nomes les dades requerides

- Procediments en tots els àmbit per la eliminació i destrucció de dades que es considerin innecessàries que, de alguna forma, així passat a traves dels controls prèviament definits

Una vegada filtrades totes les dades innecessàries, les si necessàries que identifiquen a la persona o titular en qüestió pesen per un procés de encriptació i pseudonomització removent les dades que identifiquin el titular per pseudònims a la vegada que totes aquestes dades s'encripten abans de ser emmagatzemades. Amb aquest procés ens assegurem que encara que s'arribés a tenir accés a les dades el procés de identificar el titular al que pertanyen sigui el mes complex possible.

Per evitar aquest accés, que podria ser mal intencionat, es crearan processos de restricció d'accés a tots els nivells de la empresa, registrant to accés i motiu d'aquest accessos i limitant-los nomes al personal amb autorització. Tota dada de categoria especial guardada en el sistema, com poden ser les dades mediques, tindran un nivell més de restricció on nomes amb autorització d'alt nivell a la empresa i després de la justificació i aprovació del accés es puguin consultar.

En el cas de que s'hagi de processar dades a les que no es pot aplicar aquest mètodes (dades físiques) es seguiran una sèrie de procediments extra per assegurar-ne la protecció

- Nomes es treballarà amb copies, mai amb originals.

- Les copies seran subjecte d'un filtratge per eliminar qualsevol informació innecessària d'aquestes.

- Una vegada nomes les dades pertinents quedin es passaran a un format electrònic per poder aplicar el procediments de protecció esmenant prèviament.

Per assegurar que tots aquest procediments estan actualitzats i compleixen amb la legalitat es duren a terme auditories sobre aquest anualment per avaluar i certificar el compliment de la normativa en aquest aspecte. A més d'això es reavaluara en el mateix procés la informació que es manté a la empresa per assegurar que compleix tots els requisits legals de origen, format, distribució i propietat.

Legalitat de processament

Seguint el principi definit de legalitat per la GDPR abans de processar qualsevol tipus de dades s'haurà d'establir les bases legals que ho permeten i aquestes son verificades per la regulació

En general nomes es processaran, obtindran o guardaran dades si es compleixen el requeriments legals de processament con son:

- es processarà les dades quan sigui pas necessari per a dur terme el servei del negoci o quan sigui el propi titular que ho demani.
- es processarà les dades quan sigui requeriment legal fer-ho.
- es processarà les dades si es necessari per protegir el interessos del titular
- es processarà les dades per els motius legítims de la empresa sempre i quan aquests no es sobreposin als drets del titular
- qualsevol processament tindrà que tenir el consentiment del titular

Les dades especialment protegides com poden ser dades mediques, opinió política, etc estan subjectes a una sèrie de procediments mes restrictius que fan que no es processin mai excepte si es compleixen tot els requisits com estipula el GDPR. En aquest cas les restriccions seran les següents:

- El titular de les dades ha de haver donat consentiment explícit per processar les seves dades, el consentiment implícit no es vàlid. En el específic cas de una empresa asseguradora pot sol·licitar dades especifiques, però sempre sota la limitació de ser

directament especifiques al exercici del contracte titular-empresa, tanmateix serà el titular qui ha de donar el consentiment ha compartir-les

- El processament es necessari per motius legals que estableix la necessitat de aquesta en el procés del exercici o defensa dels drets del titular en base a reclamacions legals o del jutjat

- El processament es necessari per protegir els drets del titular quan aquest no pugui donar el seu consentiment per causes físiques o legals.

Quan la empresa processi informació que cau en aquesta categoria una sèrie de procediments específics es tindran que activar per complir-ne els requisits de protecció. Aquest inclouran la necessitat de documentar qualsevol procés o tractament que es facin sobre aquestes dades a més de una justificació explícita sobre el seu us i el temps que es mantindran.

Conducta i certificació

La empresa s'adheria als codis i principis de protecció de dades, pe això els procediments i actuacions de la empresa estaran sota certificació per assegurar que aquests compleixen la llei. Per provar aquest fets la empresa es sotmetrà a auditoria i monitorització regularment i sense planejament previ assegura la major transparència possible. En cas de alguna incidència greu la empresa entén que pot perdre la certificació i, amb l'objectiu de que no passi, es revisarà anualment totes les certificacions per assegura que es compleixen els seus requisits.

Els treballadors de la empresa recolzaran aquest procediments assegurances de mantenir un reglament ètic de conducta exemplar per assegura la transparència i comptabilitat, a més de ser els últims elements asseguradors en el manteniment de la integritat de les dades.

Processament per tercers

En el cas de processament fet per tercers la empresa s'assegurarà que aquest compleixen els mateixos requisit de seguretat i protecció de dades que s'espera de la empresa mateixa. Per això abans de començar cap acció contractual per el tractament de dades requerirem sempre que la empresa de tercer passi una auditoria sobre els seus processos i activitats per assegurar que segueixen las mateixes regulacions que estipula la GDPR.

A mes de les regulacions establertes i per assegurar-nos de que es segueixen els mateixos principis de seguretat que defineixen la empresa requerirem que la empresa de tercers compleixi:

- Nomes es processarà les dades requerides.
- Qualsevol requisit legal que tingui sobre les dades serà comunicat a la empresa.
- Es prendran totes les mesures de seguretat per protegir les dades personals del titular de les dades.
- Esta sotmesa a auditories e inspeccions que asseguren el compliment de la normativa.
- En tot moment respecta els drets dels titulars de les dades.
- Informa a la empresa immediatament de qualsevol incidència o intrusió que posi en risc les dades dels titulars

Retenció i eliminació de dades

La empresa tindrà definits processos específics per assegurar que les dades nomes es mantenen el temps requerit per llei i per la GDPR que estipula que nomes s'han de mantenir el mínim de temps indispensable.

Tots els processos de eliminació que s'utilitzaran asseguren que es manté el dret a la privacitat del titulars de les dades assegurant-se que al final del procés aquestes no son recuperables (tant física com digitalment) ni que poden se utilitzades per identificar-los o extreure'n cap informació.

Procediments de drets dels titulars de les dades

Consentiment i dret a ser informat

En el mon de les assegurances la recol·lecció de dades i en especial de dades de categoria restringida es part necessària per la prestació de serveis (per exemple en cas de accident es poden requerir les dades mediques). Per aquest motiu s'han de aplicar mesures i controls específics per assegurar que les condicions de consentiment es compleixen.

- Tota petició de consentiment serà clar i transparent, utilitzant llenguatge simple i evitant tecnicismes.

- No s'utilitzaran formules amb respostes pre-omplertes.

- Cada vegada que es sol·liciti consentiment s'informarà del fet al titular de les dades de forma directa i clara.

- Juntament amb la petició de consentiment s'informarà de per a que s'utilitzarà la informació així com qualsevol tercer al que se li aplicarà el consentiment.

- Tots els procediments de consentiment seran verificables i permetran evidenciar de forma clara si el titular de les dades acceptat el tractament de les seves dades i també de que se'ls ha informat sobre com i qui utilitzarà les dades.

- Tot procés de retirada de consentiment serà processat immediatament i sense cap trava per part de la empresa.

- Tot els consentiments ja donats seran re-avaluats de forma periòdica i renovats cada vegada que hi hagi qualsevol canvi aplicable ja sigui per canvis de servei o regulació.

- Quan el consentiment apliqui sobre dades restringides aquest haurà de ser donat de forma totalment explicita i el seu us completament detallat.

Per a obtenir el consentiment l'empresa utilitzarà processos clars i documentats poden demostrar si el titular de les dades ha donat el consentiment. De la mateixa forma els processos de retirada de consentiment seguiran les mateixes regles. Els principals mètodes de acceptació de consentiment seran els següent.

- Cara a cara amb document escrit. Una vegada omplert es mourà a format digital i es guardarà una copia per motius de control.

- Per telèfon amb formulari electrònic omplert per l'atendent de la trucada. Seguint els protocols de control les trucades que continguin entrega de consentiment seran registrades com a comprovant de la entrega de consentiment.

- Electrònicament a traves de la pagina de la empresa. El procés serà similar al electrònic però serà el titular de les dades qui omplirà el formulari directament. Una vegada acceptat es registrarà al sistema.

Polítiques de privacitat

Les polítiques de privacitat de la empresa seran entregades al titular de les dades cada vegades que aquestes siguin recol·lectades independentment del format en que s'estiguin obtenint. Aquestes contindran tota la informació legal sobre el processament de les dades, incloent el motiu, duració y procés que es seguirà.

A part de en els processos de recollida les mateixes polítiques de privacitat seran accessibles a traves de la web de la empresa, en les seves oficines o es pot sol·licitat per telèfon o mail que aquestes siguin remeses al sol·licitant.

El document de polítiques de privacitat de la empresa serà redactat de forma clara i entrenadora, evitant en tot el possible de utilitzar termes no comprensibles pel públic general i detallant cada punt de forma concreta habilitant al lector a conèixer totes les implicacions i processos a que les dades recol·lectades seran sotmeses.

Dades personals no obtingudes del titular de les dades

Quan la empresa obtingui o processi dades personals que no hagin sigut obtingudes directament del titular de les dades aquesta es compromet a comunicar i entregar la informació recopilada al mateix titular dins del període estipulat de la normativa. En cas de que es produeixi la situació la empresa es compromet a comunicar el següent:

- El tipus de dades recol·lectada
- Els contingut d'aquestes dades
- L'origen del que s'han obtingut les dades

Dret d'accés

El dret de accés preveu que es tingui procediments creats per permetre un accés ràpid, concís i transparent que permeti al titular de les dades d'accedir a aquestes en qualsevol moment en un llenguatge clar i entenedor.

Aquesta informació es proporciona de forma gratuïta i està per escrit o per altres mitjans quan sigui autoritzada per l'afectat i amb la verificació prèvia de la identitat del titular.

L'entrega de les dades sol·licitades es farà en un màxim de 30 dies amb la possibilitat d'extensió per 60 dies més en el cas de dades de gran complexitat sempre que estigui justificat. En el cas de que aquesta previsió no es compleixi s'informarà al titular de les dades de les raons del enrederament o negativa d'entrega i estarà en el seu dret de registrar un queixa contra la companyia a la entitat supervisora corresponent.

Quan un titular de dades sol·licita que confirmem el estat de les seves dades personals i/o sol·licita accés a aquestes es proporcionarà la següent informació:

• El tipus i categoria al que pertany les dades processades.

• Tot subjecte al que se li ha compartit/entregat aquesta informació

• Període en que s'emmagatzemaran les dades amb els criteris utilitzats per determinar aquest període

• L'existència del dret a sol·licitar rectificació o eliminació de dades personals o el dret a demanar restriccions sobre el tractament de dades personals sobre l'interessat o oposició a aquest tractament

• El dret a presentar una queixa davant una autoritat de supervisió

• L’objectiu per el qual es processen aquestes dades

• Quan la companyia no hagi recopilat les dades personals de l’interessat, qualsevol informació disponible sobre l’origen i el proveïdor

Les sol·licituds d’accés als subjectes es transmeten al responsable de la protecció de dades tan aviat com s’ha rebut i s’observa un registre de la sol·licitud. El tipus de dades de caràcter personal que es mantenen sobre el l’individu es verifica amb l’auditoria d’informació per veure en quin format es troba, qui més ho té i amb qui s’ha compartit.

Les sol·licituds sempre es completen en un termini de 30 dies i es proporcionen de forma gratuïta. Quan l’individu realitza la sol·licitud per mitjans electrònics, es proporciona la informació utilitzant els mateixos mitjans a menys que es sol·liciti d’altra manera.

Portabilitat de dades

L’Empresa oferirà tota la informació personal que pertany a l’assumpte de dades i en un format, és fàcil de revelar i llegir. Ens assegurem que complim les dades drets de portabilitat de les persones, garantint que totes les dades personals estan disponibles i es troba en una format estructurat, usat habitualment i llegible per màquina, que permet als subjectes a obtenir i reutilitzar les seves dades personals per als seus propis fins a través de diferents serveis.

Utilitzem els formats següents per a les dades llegibles per màquina (Principalment XML):

• HTML

• CSV

• XML

• .doc / docx

• .PDF

Es realitzen totes les sol·licituds d’informació que s’ha de proporcionar a l’interessat o al controlador designat de forma gratuïta i dins dels 30 dies següents a la recepció de la sol·licitud. Si per qualsevol motiu no s’actua en resposta a una sol·licitud, es proporcionarà una explicació completa i escrita en un termini de 30 dies a l’interessat o els motius de denegació i el dret a denunciar-se davant l’autoritat de supervisió i la justícia.

Es valora totes les sol·licituds de transmissió sota el dret de portabilitat per garantir que no hi hagi cap altre titular que sigui afectat. Quan les dades personals es refereixen a més individus que el titular de les dades que les sol·licita o demani la transmissió a un altre controlador, això es farà sempre sense perjudici dels drets i llibertats de les altres persones afectades.

Rectificació i dret a la supressió de dades

Es revisaran i verificaran totes les dades que es conserven i processen per la empresa per assegurar que son exactes sempre que sigui possible i estar sempre al dia. On s'identifiquen inconsistències i / o quan l'interessat o el controlador informen que les dades que tenim no són exactes, es prendran tots els passos raonables per garantir que aquestes inexactituds es corregeixin amb efecte immediat.

Es comunicarà a la persona responsable les sol·licituds de les persones afectades per actualitzar les dades personals, validar la informació i rectificar errors quan se'ls ha notificat. La informació es modifica segons les indicacions de l'interessat, auditant la informació per garantir que s'actualitzen totes les dades relacionades amb l'assumpte incomplet o inexacte. Un cop actualitzats es pot afegir una nota o una declaració complementària on aplicable.

Quan es notifiqui les dades inexactes per part de l'interessat, es rectificarà l'error en un termini de 30 dies i s'informarà a qualsevol tercer de la rectificació si les dades personals en qüestió han sigut transmeses als mateixos en algun punt. Es comunicarà a la persona interessada per escrit la correcció i, si escau, se li subministrarà el document detalls de qualsevol tercer a qui s'hagin revelat les dades. Si per qualsevol motiu no es pot actuar en resposta a una sol·licitud de rectificació i / o finalització, sempre s'oferirà una explicació per escrit a la persona informant del dret a reclamar a l'autoritat de supervisió via un recurs judicial.

La empresa garantirà que les dades personals que identifiquin al titular de les dades no es mantenen més del que sigui necessari per a les finalitats per a les quals es processen les dades personals. Totes les dades personals obtingudes i processades per l'empresa es classificaran quan s'avaluen les dades i es dona una data d'esborrat controlant-la de manera que les dades puguin ser destruïdes quan ja no sigui necessari.

Dret a la restricció de processament

En determinades circumstàncies la empresa restringirà el processament de la informació personal, per validar, verificar o complir un requisit legal d'una sol·licitud de persones afectades. Les dades restringides s'eliminen del flux normal d'informació i es registren com a restriccions a l'auditoria d'informació. Qualsevol sistema relacionat amb el titular de les dades amb dades restringides s'actualitzarà per notificar als usuaris la categoria i la raó de restricció.

Quan les dades estan restringides, només s'emmagatzemaran de manera segura i no es processa de cap manera.

La companyia aplicarà restriccions al processament de dades en les següents circumstàncies:

• Quan una persona comunica discrepàncies amb l'exactitud de les dades personals i s'està en un procés de verificació de la seva exactitud o de la correcció d'aquestes.

• Quan una persona s'hagi oposat a la tramitació de les dades i s'estigui considerant si es te motius legítims per anul·lar els de l'individu i continuar amb la tramitació.

• Quan es considera que el tractament ha estat il·lícit, però els requisits del titular de les dades es que no s'eliminin.

• Quan ja no necessitem les dades personals, però el subjecte requereix les dades per establir, exercir o defensar una reclamació legal.

La persona responsable de la protecció de dades revisa i autoritza totes les sol·licituds i accions de restricció i conserva còpies de les notificacions dels interessats i de tercers rellevants. Quan les dades estan restringides i s'hagin divulgat aquestes dades a un tercer, s'informarà a la tercera part de la restricció establerta i de la raó informant si es trenca alguna d'aquestes restriccions.

Els interessats que han sol·licitat la restricció de les dades rebran resposta en un termini de 30 dies després de l'aplicació de restricció i també es comunicarà a qualsevol tercer a qui s'hagin revelat les dades. També es proporcionarà per escrit a l'interessat qualsevol decisió d'aixecar una restricció al processament. Si per qualsevol motiu no s'és capaç d'actuar en resposta a una sol·licitud de restricció, sempre es proporcionarà una explicació per escrit a la persona i seran informats del seu dret a queixar-se davant l'Autoritat de Supervisió i a un recurs judicial.

Objeccions i decisions automatitzades

S'informarà als interessats del seu dret a oposar-se al tractament de dades en els avisos de privadesa i en el moment de la primera comunicació, de forma clara i llegible i separada de la resta d'informació. Oferirà opcions de renúncia a tot el material de màrqueting directe i es proporcionarà un formulari d'objecció en línia on es realitza el processament si e necessaru. Els individus tenen dret a oposar-se a:

• Processament de la seva informació personal basada en interessos legítims o en la realització d'una tasca en l'interès públic

• Màrqueting directe

• Processament per a finalitats de recerca i estadística científica

Quan l'empresa processa les dades personals per a l'execució d'una tasca legal, en relació amb els interessos legítims o amb finalitats de recerca, l'objecció d'un interessat només es tindrà en compte quan es tracti de motius relacionats amb la seva situació particular. Es reserva el dret de continuar processant aquestes dades personals quan:

• Es poden demostrar motius legítims i convincents per al tractament, que anul·len els interessos, drets i llibertats de la persona.

• El processament és per a l'establiment, l'exercici o la defensa de reclamacions legals en què s'està processant informació personal.

Quan s'està processant informació personal amb finalitats de màrqueting directe sota un consentiment obtingut prèviament, es deixarà de processar aquestes dades personals immediatament quan una objecció sigui rebuda de l'interessat. Aquesta mesura és absoluta, gratuïta i sempre respectada.

Quan una persona objecte el tractament de dades per motius vàlids, l'empresa cessarà el tractament per a aquest propòsit i avisarà l'interessat per escrit d'aquest cessament en els 30 dies següents a la recepció de l'oposició.

Es farà una auditoria de sistemes per identificar processos de presa de decisions automatitzats que no impliquen intervenció humana. També s'avaluaran nous sistemes i tecnologies per a aquest mateix component abans de la seva implementació. Les decisions absents de les interaccions humanes poden estar esbiaixades cap a les persones d'acord amb el GDPR per lo que s'hauran de posar en marxa mesures per salvaguardar les persones i les seves dades. Mitjançant els avisos de privadesa, en les primeres comunicacions amb una persona es recordarà als individus els seus drets a no ser objecte de decisió quan:

• Es basa en un processament automatitzat

• Produeix un efecte jurídic o un efecte similar a l'individu

En circumstàncies limitades, l'empresa utilitzarà processos de presa de decisions automatitzats dins de les directrius de la normativa. Aquestes instàncies inclouen:

• On és necessari per dur a terme o dur a terme un contracte entre l'empresa i l'individu

• On està autoritzat per la llei

• Quan es basi en el consentiment explícit per fer-ho

• Quan la decisió no té cap efecte legal o similarment significatiu en algú

Quan l'empresa utilitza processos de presa de decisions automatitzats, sempre s'informarà a la persona i els assessors dels seus drets. També assegurarà que les persones poden obtenir intervenció humana (tractar amb un representant de la empresa), expressar el seu punt de vista i obtenir una explicació de la decisió que s'ha pres i desafiar-la en cas de que l'individu consideri que vulnera els seus drets.

Procediments de supervisió

Juntament amb les polítiques de protecció de dades personals, assegurarà la màxima seguretat de les dades que es processen, incloent-hi com a prioritat, quan es comparteixen, es divulguen i es transfereixen. Les polítiques de seguretat de la informació proporcionaran les mesures detallades i els controls que s'han d'adoptar per protegir la informació personal i garantir la seva seguretat des del consentiment fins a la seva eliminació.

Es realitzaran auditories d'informació per assegurar que totes les dades personals que es tinguin i/o es processin per la empresa siguin comptabilitzades i registrades, juntament amb les avaluacions de riscos sobre l'abast i l'impacte que pot tenir una infracció de dades sobre els titular de les dades. S'hauran d'implementar mesures tècniques i organitzatives adequades per garantir un nivell de seguretat adequat al risc.

La empresa es comprometrà a fer tots els esforços necessaris per a reduir el risc d'infraccions sobre les dades i haurà de disposar de controls i procediments dedicats per a aquestes situacions, juntament amb les notificacions que s'hauran de fer a l'autoritat de control i als interessats.

Compartiment i transferència de dades

L'Empresa adoptarà mesures proporcionals i efectives per protegir les dades personals que es tinguin i processin en tot moment, reconeixent la naturalesa d'alt risc de la divulgació i transferència de dades personals i posant una prioritat encara més gran en la protecció i seguretat de les dades.

Les transferències de dades dins de la UE es consideren menys perilloses que a un tercer país o una organització internacional a causa de les lleis de protecció de dades que cobreixen les primeres i les estrictes normes aplicables a tots els estats membres de la UE. Quan es transfereixen dades per a una finalitat legal i necessària, conforme a tots els articles del GDPR, utilitzarà un procés que garanteixi que aquestes dades es xifren amb una clau secreta i, si és possible, també estan subjectes als mètodes de minimització de dades.

S'utilitzaran mètodes de transferència segurs i aprovats i es disposarà de punts de contacte específics amb cada organització d'Estat membre amb qui es faci la transferència/comunicació. Per totes les dades que es transfereixin aquestes s'anotaran a la auditoria d'informació perquè el seguiment estigui fàcilment disponible i l'autorització sigui accessible. El responsable de la protecció de dades autoritzarà totes les transferències de la UE i verifica els mètodes de xifratge, seguretat i mesures.

Auditories y monitorització

Es realitzaran auditories regulars i processos de seguiment de la conformitat que es detallaran a la política de la empresa juntament amb els procediment de seguiment finalitzant en una auditoria de compliment, amb la finalitat de garantir que les mesures i els controls existents per protegir els interessats i la informació siguin adequats, eficaç i conforme amb la normativa en tot moment.

El responsable de la protecció de dades tindrà la responsabilitat general d'avaluar, provar, revisar i millorar els processos, mesures i controls existents i informar els plans d'acció de millora a l'equip directiu. Els mètodes de minimització de dades seran freqüentment revisats i les noves tecnologies seran avaluades per garantir que s'està protegint les dades i persones de la millor manera possible.

El responsable de la protecció de dades registrarà totes les revisions, auditories i processos de seguiment continuats. A més es facilitaran còpies d'aquests a la Direcció i es posaran tambe a disposició de l'Autoritat de supervisió quan sigui necessari. L'objectiu de les auditories internes de protecció de dades serà:

• Assegurar que hi hagi les polítiques i procediments adequats

• Verificar que aquestes polítiques i procediments s'aconsegueixen

• Provar l'adequació i l'eficàcia de les mesures i controls vigents

• Per detectar incompliments o possibles incompliments del compliment

• Identificar els riscos i avaluar les accions de mitigació establertes per minimitzar aquests riscos

• Recomanar solucions i plans d'acció a l'Alta Direcció per millorar la protecció de les persones afectades i la salvaguarda de les seves dades personals

• Fer el seguiment del compliment de les lleis de protecció de dades i demostrar les millors pràctiques.

Entrenament i preparació

La empresa haurà d'assegurar que tot el personal entengui, tingui accés i pugui interpretar fàcilment els requisits de les lleis de protecció de dades i els seus principis a més de que tinguin formació, suport i avaluacions contínues per garantir i demostrar el seu coneixement, competència i adequació. Les polítiques i procediments de formació i desenvolupament i la política de inducció detallaran com es formen, avaluen i donen suport als empleats nous i existents incloent:

• Tallers i sessions de formació de GDPR

• Proves d'avaluació per demostrar-ne la seva comprensió

• Coaching & Mentoring per part dels càrrecs de gestió d'equips per els nous integrants.

• Sessions de suport cara a cara per qualsevol dubte sobre la normativa

• Recordatoris i avisos automatitzats si escau

• Accés a polítiques, procediments, llistes de comprovació i documents de suport de GDPR. Els empleats estan sempre recolzats i formats en les lleis de protecció de dades i als objectius i obligacions propis de la protecció de dades.

Infraccions

L'empresa atindrà a les seves obligacions i responsabilitats segons les lleis de protecció de dades reconeixent la gravetat de violar qualsevol part de la llei o el Reglament. Es respectarà l'autorització de l'Autoritat Supervisora segons la legislació per imposar i aplicar multes i sancions quan no es compleixi la normativa, no aconsegueixi mitigar els riscos quan sigui possible, operar de manera inconscient i/o no conforme amb la normativa. Els empleats hauran de ser conscients de la gravetat d'aquestes sancions i de la seva naturalesa proporcional, de conformitat amb l'incompliment.

• Les infraccions de les obligacions del responsable del control, del processador, de l'entitat de certificació i de l'entitat de control, estaran subjectes a multes administratives de fins a 10.000.000 d'euros.

• Infraccions dels principis bàsics per al processament, les condicions del consentiment, els drets de les persones afectades, les transferències de dades personals a un destinatari en un país tercer o en una organització internacional, situacions de processament específiques o incompliment d'una comanda per L'Autoritat de Supervisió està subjecta a multes administratives de fins a 20.000.000 €.

Responsabilitats

La Companyia ha de designar un responsable de protecció de dades el paper de la qual és identificar i mitigar qualsevol risc per a la protecció de dades personals, actuar de manera consultiva per a l'empresa, els seus empleats i els alts càrrecs i per mantenir la empresa i activament informada i actualitzada amb tota la legislació i els canvis relacionats amb la protecció de dades.

El RPD treballarà conjuntament amb el responsable de compliment, el responsable de TI i el responsable de formació per garantir que tots els processos, sistemes i personal funcionin de manera compatible i amb els requisits de les lleis de protecció de dades i els seus principis.

El RPD tindrà la responsabilitat global amb la deguda diligència de les avaluacions d'impacte de la privadesa, l'anàlisi de riscos i les transferències de dades quan s'hi impliquen dades personals i també mantindran informes de gestió i registres adequats i efectius d'acord amb les lleis de protecció de dades i els nostres propis objectius i obligacions internes.

El personal que gestioni i processi informació personal o de la categoria especial haura de rebre una formació de protecció de dades extensa i estarà subjecta a un suport continuat de desenvolupament i tutoria per assegurar-se que són competents i coneixen el paper que duen a terme.

Conclusions

El GDPR està dissenyat per protegir més les dades personals de les persones. Això requerirà una inversió significativa de temps i diners. No obstant això, aquests canvis també permetran a les empreses pensar amb més atenció sobre com interactuen amb els seus clients i, a llarg termini, poden millorar les relacions amb els clients amb una major confiança i un respecte per la privadesa personal.

El compliment de GDPR no és un problema a prendre a la lleugera, No només imposa dures sancions a les organitzacions que descuiden la protecció de dades personals i la privadesa de l'usuari, sinó que també planteja riscos greus quant a imatge de l'empresa, afecta la competitivitat de l'empresa al mercat i la qualitat general dels serveis que proporciona.

Tanmateix, les organitzacions no han de considerar aquesta regulació com a estipulació, sinó com una oportunitat per obtenir un avantatge sobre els competidors en el futur mercat completament regulat, basar-se en la fidelitat i la confiança dels clients i millorar els seus sistemes de gestió de dades.

Per a empreses que no tinguin una gran clientela a la UE, és clar que les implicacions del GDPR són menys clares. No obstant això, mentre que les organitzacions que no siguin comunitàries a la UE no hauran de preocupar-se immediatament pel compliment de GDPR en les seves pròpies pràctiques, és poc probable que estiguin totalment protegits dels efectes de la regulació. A curt termini, per exemple, els mercats que no pertanyen a la UE poden veure un afectats, ja que la complexitat de la regulació i les preocupacions sobre el compliment i la responsabilitat temporal fan que els mercats menys regulats siguin més atractius.

Annex

CDT guia per el GDPR

El següent document es un extracte resumit de la guia per el compliment del GDPR d'una empresa que anomenarem CDT i dedicada a la implementació de software per asseguradores.

Resum executiu

Els proveïdors d'assegurances s'estan preparant per a nous requisits reglamentaris que entraran en vigor el maig del 2018 en virtut del Reglament general de protecció de dades (GDPR). El propòsit de la regulació és protegir les dades personals dels residents de la UE a mesura que participin en activitats i transaccions en línia. Aquesta guia de CDT analitza les disposicions selectes del GDPR per proporcionar informació addicional als nostres clients subjectes a la normativa.

Compliment de les normes de privadesa de dades

CDT dona suport als proveïdors d'assegurances de tot el món, que estan subjectes a requisits reglamentaris locals específics. A mesura que es desenvolupen mesures com el GDPR i els organismes reguladors estableixen registres de seguiment (per exemple, el grup de treball Article 29, l'ICO del Regne Unit), CDT controla aquestes fonts, així com publicacions de la indústria i canals de comentaris dels clients, per respondre a qualsevol canvis necessaris. Ens comprometem a oferir funcions i productes que proporcionin les eines que permeten als proveïdors d'assegurances mantenir el compliment d'aquests reglaments importants.

Per garantir el compliment normatiu, els proveïdors d'assegurances es basen en grups i processos interns per controlar i avaluar els canvis normatius, com els que requereix el GDPR. Aquests grups recopilen informació de fonts de la indústria per informar de les seves perspectives sobre com els proveïdors d'assegurances es refereixen al compliment normatiu. Quan s'identifiquen els canvis necessaris, els proveïdors d'assegurances utilitzen el programari de CDT per configurar les regles, els processos i els fluxos de treball necessaris per aconseguir el compliment normatiu.

Preparació per a la identificació i classificació de dades

Com a part de la implementació inicial del compliment de GDPR i com a part de les activitats de manteniment posteriors, els proveïdors d'assegurances han d'identificar i classificar elements de dades personals, la majoria dels quals s'utilitzen en diversos sistemes (tant CDT com no CDT). El catàleg resultant d'elements de dades es pot consolidar en un inventari de dades a tot l'empresa, que dona suport a les capacitats permanents de:

- Cercar i identificar dades personals
- Facilitar la classificació de dades
- Mantenir un inventari dels fons de dades personals

L'inventari de dades resultant del proveïdor d'assegurança proporciona la base per donar suport als drets individuals de cadascun dels subjectes de dades, que són parts clau dels principis de protecció de dades de GDPR. Per recolzar les activitats de classificació i identificació de dades d'un proveïdor d'assegurances, CDT proporciona un inventari de dades personals per identificar i descriure les dades personals emmagatzemades, processades i transmeses per les solucions de CDT. A més, la nova característica de Microsoft Data Discovery & Classification, publicada el 15 de febrer de 2018, hauria de ser considerada com una eina per donar suport a aquests esforços. Utilitzant una o altra eina, els proveïdors d'assegurances mantenen un inventari actualitzat de tots els elements de dades personals, les ubicacions de l'empresa i les classificacions reguladores necessàries.

Drets individuals i obligacions empresarials

Els principis de protecció de dades de GDPR estan formats per un conjunt de drets individuals (per als titulars) i un conjunt relacionat d'obligacions de l'empresa (per als controladors de dades i els processadors). Aquesta guia revisa els següents drets i obligacions:

- El dret a ser informat
- El dret d'accés
- El dret a la rectificació
- El dret a l'esborrat
- El dret a restringir el processament

- El dret a la portabilitat de dades
- Drets relacionats amb la presa de decisions automatitzada
- L'obligació de proporcionar protecció de dades per disseny i per defecte

Cada dret es revisa a continuació en termes de com es caracteritza dins del GDPR i de les maneres en què els nostres clients implementen CDT per donar suport a cada principi.

El dret a ser informat

El GDPR requereix que els proveïdors d'assegurances proporcionin:

- "Informació de processament just", normalment mitjançant un avís de privadesa
- Transparència sobre com s'utilitzen les dades personals

El dret a ser informat es destaca l'obligació del proveïdor d'assegurança de proporcionar un mecanisme de comunicació (és a dir, un avís de privadesa de dades) que descrigui clarament com utilitza les dades personals d'un subjecte de dades a tota la seva empresa. Aquest avís de privadesa ha d'explicar clarament totes les activitats de processament que utilitzen dades personals i si aquestes activitats són iniciades pel proveïdor d'assegurances o els seus processadors de tercers. El proveïdor d'assegurança normalment proporciona l'avís de privadesa al subjecte de dades abans de l'inici de les activitats de processament. L'Inventari de dades personals de CDT i la documentació de trets en línia al Centre de solucions haurien d'utilitzar-se per contribuir a les descripcions d'activitats de processament detallat necessàries per a cada element de dades personals.

El dret d'accés

El dret d'accés garanteix que l'interessat pugui:

- Accedir a les seves dades personals i informació complementària
- Conèixer i verificar la legalitat del processament

CDT ofereix un conjunt complet de pàgines d'aplicació i capacitats del sistema que faciliten la cerca, el processament i la presentació d'informes de dades personals. A més de les riques capacitats que ofereix, el proveïdor d'assegurances utilitza les eines de configuració de CDT per crear i exposar opcions addicionals de punts d'accés, processos i informes per donar suport al dret d'accés de l'interessat.

Com a part de la realització de l'Inventari de dades personals de CDT, el proveïdor d'assegurança estableix la legalitat del processament descrivint el motiu pel qual es requereix el procés. Aquesta justificació legal ha d'estar disponible a l'avís de privadesa de dades de clients, per a consultes dels clients sobre l'ús acceptable i per a sol·licituds de suspendre o suspendre el processament.

El dret a la rectificació

Com el proveïdor d'assegurança recopila dades sobre un subjecte de dades, el GDPR:

- Assegura que les persones poden tenir dades correctes o incompletes corregides

El sol·licitant de correcció o realització de dades és processat pel proveïdor d'assegurances a la pàgina d'aplicació relacionada amb CDT, utilitzant normes comercials automatitzades o utilitzant les API de CDT. El proveïdor d'assegurances pot confirmar automàticament els canvis amb les normes de negoci configurades o amb la notificació proporcionada als processadors de tercers a través de les integracions implementades de CDT.

El dret a l'esborrat

El dret a l'esborrat requereix que el proveïdor d'assegurances localitzi i esborri dades personals a petició. Aquest dret es coneix com a "dret a ser oblidat" i permet a un individu:

- Sol·liciteu la supressió o eliminació de dades personals quan no hi hagi motius convincents per al seu processament continuat.

Un cop que el proveïdor d'assegurances hagi completat l'Inventari de dades personals, l'inventari conté les ubicacions de tots els elements de dades personals, ja siguin ubicats a la base de dades d'aplicacions de CDT, en fitxers o als servidors. El proveïdor d'assegurances utilitza les ubicacions registrades a l'Inventari de dades personals per identificar i esborrar les dades personals d'un subjecte de dades, ja sigui com a part d'una pàgina d'aplicació configurada o per un procés automatitzat. CDT compartirà tots els patrons d'aplicació comuns per a aquelles pàgines d'aplicacions o processos automatitzats a mesura que s'ofereixin

El dret a restringir el processament

Les persones interessades tenen el dret de sol·licitar que el seu proveïdor d'assegurances deixi o restringeixi qualsevol processament que utilitzi les seves dades. Aquest dret especifica que:

- Les persones tenen dret a "bloquejar" o suprimir el processament de dades personals

- Quan el processament està restringit, es pot emmagatzemar les dades personals, però no utilitzar-lo per a processaments posteriors
- Només es pot conservar prou informació sobre la persona per garantir que es respecti la restricció en el futur.

Després que el proveïdor d'assegurances hagi completat l'Inventari de dades personals, l'inventari identifica i descriu les capacitats de referència i les capacitats específiques de la implementació per interrompre i restringir el processament de dades personals. Per complementar la documentació de configuració creada pel proveïdor d'assegurances durant la implementació, CDT ofereix una àmplia documentació de característiques a través del Centre de solucions en línia, que descriu les capacitats proporcionades per la base per suspendre i restringir el processament. Per enregistrar i aplicar la sol·licitud de restricció de procés, les aplicacions de CDT permeten gravar notes de contacte, per exemple, notes de política, notes de comptes de factures i notes de fitxers de reclamacions.

Els proveïdors d'assegurances també utilitzen les eines de configuració de CDT per afegir normes de flux de treball que eviten les activitats de processament de dades fins que rebin el consentiment granular i inequívoc de la persona afectada. Per exemple, els proveïdors d'assegurances utilitzen l'eina de configuració de l'autor de CDT per afegir una regla al flux de treball de cotització que impedeix que l'usuari processi la cita fins que l'interessat doni el seu consentiment.

El dret a la portabilitat de dades

El proveïdor d'assegurança ha de proporcionar als interessats les seves dades personals en un format estructurat i comú perquè puguin:

- Obtenir i reutilitzar les seves dades personals per als seus propis fins a través de diferents serveis
- Moure, copiar o transferir les seves dades personals de manera senzilla des d'un entorn informàtic a un altre de manera segura i segura, sense impedir la facilitat d'ús.
- Aprofiteu les aplicacions i serveis que poden utilitzar aquestes dades per trobar-los millor, o ajudar-los a entendre els seus hàbits de despesa

Utilitzant les ubicacions registrades a l'Inventari de dades personals, el proveïdor d'assegurança identifica totes les instàncies de les dades personals i les presenta en una pàgina d'aplicació, lletra o informe configurada. Com a resposta a les sol·licituds dels subjectes de dades sobre les seves dades personals, es poden proporcionar les dades en qualsevol d'aquests formats habituals i de fàcil comprensió. Els formats habituals configurats durant les implementacions inclouen un formulari imprès (p. Ex., Utilitzant formularis de CDT) o un informe integrat que fa que les dades siguin necessàries (per exemple, en XML o Excel).

Drets relacionats amb la presa de decisions automatitzada

Els proveïdors d'assegurances han d'identificar les decisions o processos realitzats totalment o parcialment per mitjans automatitzats. Atès que el proveïdor d'assegurances ha de revelar (per exemple, a través de l'avís de privadesa) com s'utilitzen les dades sensibles, aquesta disposició:

- Proporciona salvaguardes a les persones contra el risc que es prengui una decisió potencialment perjudicial sense la intervenció humana (la presa de decisions, incloent el perfilat)

A la documentació disponible de l'empresa CDT identifica i descriu els processos proporcionats per la base del programari i els elements de dades personals implicats. A l'execució, el proveïdor d'assegurances completa l'Inventari de dades personals juntament amb la documentació de configuració de característiques. Quan s'utilitzen junts, aquestes referències proporcionen descripcions lògiques de com els processos automatitzats del proveïdor d'assegurança usen dades personals a CDT.

Protecció de dades per disseny i per defecte

Els proveïdors d'assegurances tenen l'obligació de crear i mantenir un pla a escala de l'empresa per desenvolupar tecnologia, productes, processos i una estructura organitzativa amb protecció de dades i privadesa com a components integrals. El GDPR subratlla que:

- Les empreses tenen l'obligació general d'implementar mesures tècniques i d'organització per mostrar la seva consideració i integració en les seves activitats de processament.

CDT i les tecnologies de la plataforma subjacents ofereixen les eines necessàries perquè els proveïdors d'assegurances compleixin la normativa de privadesa de dades. Aquests poden incloure:

- Permisos d'usuari i permís d'autenticació, que permeten un subconjunt restringit d'usuaris accedir o modificar dades personals (per exemple, Administració d'usuaris).

- El xifratge de dades personals en repòs utilitzant el xifratge a nivell de volum mitjançant BitLocker i Microsoft Transparent Data Encryption (TDE), per a MS SQL Server o Azure Server.

- Ús de TLS / SSL i IPsec per al xifratge de dades en viu.

- Emmascarament de dades o ofuscament.

Conclusións

Els clients de CDT gestionen negocis a tot el món i han de complir els requisits reglamentaris aplicables, com els especificats al GDPR. Com a proveïdor de programari d'assegurances bàsic, CDT té un compromís constant de construir capacitats aplicables a nivell mundial que permetin als proveïdors d'assegurances complir amb les seves obligacions reguladores locals i els requisits de compliment. Amb aquesta finalitat, a mesura que els proveïdors d'assegurances utilitzen les eines de programari de CDT per configurar les regles, processos i fluxos de treball requerits, CDT fomenta una relació estreta amb l'equip local i l'administrador de comptes per a qualsevol ajuda que CDT pugui oferir.

Bibliografia

Judy Schmitt, Florian Stahl. 11/11/2012. How the Proposed EU Data Protection Regulation Is Creating a Ripple Effect Worldwide.
https://iapp.org/media/presentations/A12_EU_DP_Regulation_PPT.pdf

Cuijpers, C., Purtova, N., & Kosta, E. 2014. Data Protection Reform and the Internet: The Draft Data Protection Regulation.
https://papers.ssrn.com/sol3/delivery.cfm/ssrn_id2373683_code599.pdf?abstractid=2373683&mirid=1

Victor, J. M. 2013. The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. Yale Law Journal, 123(2), 5.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2317903

Liapakis, Xenofon. 2018. A GDPR Implementation Guide for the Insurance Industry. IJRQEH 7.4 34-44. https://www.igi-global.com/article/a-gdpr-implementation-guide-for-the-insurance-industry/211950

W. Gregory Voss. 07/2017. First the GDPR, Now the Proposed ePrivacy Regulation. Journal of Internet Law, Vol. 21, No. 1, pp. 3-11
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3008765

Simon Cooper. Mehmet Achik-El. 04-04-2018. Is the Insurance industry prepared for GDPR? Insurance, GDPR and UK Data Protection https://www.incegdlaw.com/en/knowledge-bank/is-the-insurance-industry-prepared-for-gdpr

Valarie King-Bailey. 18-12- 2018. Mastering EU GDPR Compliance: Security and Privacy for Validated Systems. http://www.ivtnetwork.com/article/mastering-eu-gdpr-compliance-security-and-privacy-validated-systems

Alan Calder. 06/2016. Preparing for EU GDPR. IT Governance Ltd
https://www.itgovernance.eu/download/preparing-for-the-eu-gdpr-june-2016.pdf

Salah Addin ElShekeil. Saran Laoyookhong. 2017. GDPR Privacy by Design. Stockholm university.
https://dsv.su.se/polopoly_fs/1.351720.1507815130!/menu/standard/file/Stipendie2017_ElShekeil-Laoyookhong.pdf