

: kritēriju saraksts

Lai nodrošinātu dokumentu un datu drošību, izvēloties e-paraksta risinājumu, ir svarīgi pievērst uzmanību vairākām lietām. Šajā kritēriju sarakstā ir atrodamas svarīgākās lietas, kurām jāpievērš uzmanība.

01 Juridiski saistoši e-paraksti

Saskaņā ar eIDAS regulu, kas nosaka elektronisko parakstu izmantošanu Eiropā, tikai kvalificēti e-paraksti ir līdzvērtīgi ar roku veiktiem parakstiem, un tikai tiem ir neapstrīdams juridiskais spēks. Pārliecinieties, ka e-paraksta nodrošinātājs ļauj izveidot un validēt e-parakstus ar kvalificētiem sertifikātiem, kas atbilst "eIDAS" regulējumam, bez jebkādiem papildu nosacījumiem, piemēram, atsevišķiem maksājumu plāniem, kas paredzēti tikai šādiem parakstiem, ierobežotu programmatūras darbību, kas darbojas tikai uzņēmuma iekšējās sistēmās, ierobežotiem e-identifikācijas rīkiem un tamlīdzīgi. Šādi papildu nosacījumi parasti nozīmē, ka ne visi pakalpojumu sniedzēja piedāvātie pakalpojumi atbilst augsta līmeņa elektroniskajiem parakstiem. Pārliecinieties, ka pakalpojumu sniedzējs tik tiešām ievēro visas "eIDAS" regulā noteiktās saistības.

02 Kvalificēti laika zīmogi

Lai pārliecinātos par to, ka dokumenti ir drošībā un nav viltošanas riska, apsveriet iespēju izmantot tikai tādu pakalpojumu sniedzēju, kas visu dokumentu parakstīšanas procesos izmanto kvalificētu laika zīmogu. Tas ļaus izvairīties gan no dokumentu, gan no parakstīšanas datumu viltošanas.

03 Parakstu ilgtermiņa derīgums

Elektroniskajiem parakstiem ir noteikts derīguma termiņš. Lai garantētu to uzticamību, pārbaudiet, vai pakalpojumu sniedzējs piedāvā ilgtermiņa uzglabāšanas pakalpojumus. Tikai tā pēc vairākiem gadiem nebūs jāsatraucas par to, ka jāmeklē papildus pakalpojumu sniedzējs, kas to nodrošina, un ka parakstītie dokumenti joprojām ir derīgi.

05 Informācijas drošības pārvaldība

Tikai kvalitatīvi veikta informācijas drošības pārvaldība var nodrošināt datu pilnvērtīgu aizsardzību. Svarīgi ir izvēlēties elektroniskās parakstīšanās pakalpojumu sniedzēju, kas piedāvā individuālu informācijas drošības pārvaldības sistēmu, ko pārbaudījuši un sertificējuši neatkarīgi akreditēti auditori. Dažreiz pakalpojumu sniedzēji izmanto datu centrus ar izveidotām uzticamības garantēšanas programmām, tomēr tās nekādā veidā nenosaka paša pakalpojumu sniedzēja informācijas drošības pārvaldības praksi.

04 Augsta pakalpojumu pieejamība

Pakalpojumu pieejamība un to sīks izklāsts var norādīt uz to, vai pakalpojumu sniedzējs ir apņēmības pilns nodrošināt pakalpojumu uzraudzību un pastāvīgu darbību. Tas ir svarīgi, lai garantētu klienta darbību nepārtrauktību. Jo augstāka būs nodrošināto pakalpojumu pieejamība un, īpaši, informācija par tiem, jo mazāk būs jāuztraucas, ka pakalpojumu izmantošanas laikā varētu rasties kādas neparedzētas problēmas. Ir svarīgi arī novērtēt pakalpojumu sniedzēja atbildību - kādas darbības ir paredzamas un kompensācija, ja pakalpojums nedarbojas.

06 Caurspīdīgums

Caurspīdīgums – tā ir uzticamība. Pārbaudiet, kāda veida informācija par pakalpojumu sniedzēju ir pieejama publiski. Sevišķi uzmanību vajadzētu pievērst trešo pušu izsniegtajiem sertifikātiem, piemērotības sertifikātiem, audita ziņojumiem, datu apstrādes politikai un citiem juridiskajiem dokumentiem. Jo vairāk informācijas uzņēmums piedāvā publiskai apskatei, jo caurspīdīgāks tas ir. Tas palīdz pārliecināties par to, ka uzņēmumam nav nekā slēpjama, un atbildīgās personas nesniedz nepatiesu informāciju par savām darbībām.

07 Kvalificēts validācijas pakalpojums

Ja plānojat izmantot elektronisko parakstu, nepieciešams arī pārliecināties par to, vai ir iespējams pārbaudīt to derīgumu. Tāpēc labāk izvēlēties risinājumu, kam ir iebūvēta elektronisko parakstu validācijas funkcija vai kurš var šim nolūkam piedāvāt papildus pakalpojumu. Ir svarīgi pārliecināties par to, vai izvēlētais pakalpojumu sniedzējs ir atbildīgs par paraksta validācijas procesu un tā rezultātiem – pārbaudiet uzņēmuma parakstu apstiprināšanas politiku, pienākumus un noteiktās saistības. Tā kā elektronisko parakstu un zīmogu validācija tiek kontrolēta un regulēta, izvēlieties kvalificētu un "eIDAS" sertificētu pakalpojumu sniedzēju. Regula nosaka, ka pilnībā var uzticēties tikai kvalificētiem parakstu validācijas pakalpojumu sniedzējiem.

09 Pozitīva lietotāju pieredze

Ja esat gatavs pievērsties digitālajam parakstīšanās risinājumam, ir jāpārliecinās par to, vai izvēlētais pakalpojumu sniedzēja sistēma ir lietotājam draudzīga. Ne mazāk svarīgi ir - vai tā darbojas vairākās operētājsistēmās un ierīcēs. Tādējādi nebūs regulāri jāmeklē lietošanas rokasgrāmata un nepieciešamās darbības būs iespējams veikt operatīvi un bez aizķeršanās. Šis ir īpaši svarīgi, ja izvēlētajā platformā ir plānots ievākt arī klientu parakstus. Šādu funkciju noteikti vajag pieprasīt - tā palīdzēs nodrošināt veiksmīgāku klientu apkalpošanu.

11 Pakalpojumu sniedzēja reputācija

Viss iepriekšminētais ir pierādījums tam, ka esat atraduši stabilu un piemērotu pakalpojumu sniedzēju, taču ne mazāk svarīgi ir pārliecināties par uzņēmuma reputāciju. Par to var liecināt uzņēmuma klientu saraksts un pieejamās atsauksmes.

08 Dokumentu formātu un e-identifikācijas rīku dažādība

Pirms izvēlēties elektroniskās parakstīšanās un parakstu uzglabāšanas pakalpojumu sniedzēju, pārbaudiet, kāda formāta dokumentus konkrētais uzņēmums pieņem. Lai gan Eiropā dokumentiem ir starptautiski atzīts formāts, katrai valstij ir arī savs individuālais formāts. Ir svarīgi pārliecināties par to, ka pakalpojumu sniedzējs atbalsta dažādus e-identifikācijas rīku formātus – tas var noderēt situācijās, kad jāparaksta kāds starptautiska partnera iesniegts dokuments.

10 Atbilstība uzņēmuma vajadzībām

Lai cik drošs un vispārpieņemtiem nosacījumiem atbilstošs būtu pakalpojumu sniedzēja piedāvātais risinājums, svarīgi ir pārliecināties, vai izvēlētajam pakalpojumu sniedzējam ir tas, kas nepieciešams uzņēmumam, neatkarīgi no tā, vai tas ir mākonī bāzēts risinājums vai integrēts uzņēmuma sistēmās, kā arī papildu funkcijas, piemēram, organizācijas stila pielāgošana, darbplūsmas vai dažādi dokumentu formāti.

SALĪDZINIET E-PARAKSTU RISINĀJUMU NODROŠINĀTĀJUS

Izmantojiet šo tabulu, lai ērti salīdzinātu savus atlasītos e-parakstīšanas pakalpojumu sniedzējus.



Juridiski saistoši e-paraksti	<p>Dokobit darbojas tikai ar:</p> <ul style="list-style-type: none">• Kvalificētiem elektroniskajiem parakstiem, kuriem ir tāds pats juridiskais spēks kā parakstiem ar roku• Uzlabotiem elektroniskajiem parakstiem ar valificētiem sertifikātiem, kas tiek uzskatīti par stingriem pierādījumiem tiesā		
Kvalificēti laika zīmogi	<ul style="list-style-type: none">• Dokobit katrā dokumenta parakstīšanā izmanto kvalificētus laika zīmogus		
Parakstu ilgtermiņa derīgums	<ul style="list-style-type: none">• Dokobit ir viss nepieciešamais, lai vajadzības gadījumā nodrošinātu visu dokumentu elektronisko parakstu ilgtermiņa saglabāšanu		
Augsta pakalpojumu pieejamība	<ul style="list-style-type: none">• Pakalpojumu pieejamība nav zemāka par 99,95%• Pakalpojumu pieejamības vēsturi var apskatīt šeit• Pakalpojumu pieejamības uzraudzību nodrošina neatkarīga uzraudzības programmatūra Pingdom• Dīkstāves gadījumā Dokobit piemēro atlaides ikmēneša rēķinam (tiek piemēroti papildu nosacījumi)		

Informācijas drošības pārvaldība

- Dokobit ir ieviesta **informācijas drošības pārvaldības sistēma**
- **ISO/IEC27001 sertifikāts** ar sertifikācijas jomu "mākoņpakalpojumi e-parakstīšanai, e-zīmogošanai, e-identifikācijai, e-paraksta un e-zīmoga validācijai un ar to saistītās programmatūras izstrādei, piegādei un atbalstam". Sertifikāts pieejams [šeit](#)
- Dokobit informācijas drošības pārvaldības sistēma atbilst Eiropas standartam **ETSI EN 319 401**, kas ir obligāts kvalificētiem uzticamības pakalpojumu sniedzējiem
- Dokobit **katru gadu auditē** divi pasaulē atzīti auditoruzņēmumi: Bureau Veritas (ISO sertifikācijai) un CSQA (ETSI sertifikācijai)

Caurspīdīgums

- **ISO/IEC27001 sertifikāts** pieejams [šeit](#)
- **Pēc pieprasījuma** tiek izsniegts **paziņojums par piemērojamību** (angl. certification statement of applicability)
- **Pakalpojumu pieejamība** pieejami [šeit](#)
- **Apdrošināšanas sertifikāts** pieejams [šeit](#)
- **Visi juridiskie dokumenti** (Pakalpojumu noteikumi, Datu apstrādes līgums, Privātuma politika utt.) pieejami [šeit](#)

Kvalificēts validācijas pakalpojums

- **Kvalificēts uzticamības pakalpojumu sniedzējs**, kuru pārrauga dalībvalsts uzraudzības iestāde (Communications Regulatory Authority of the Republic of Lithuania) un kurš ir iekļauts **ES uzticamo pakalpojumu sarakstā** (skat. [šeit](#))
- **Kvalificēta uzticamības pakalpojumu sniedzēja sertifikāts** pieejams [šeit](#)
- **Parakstu validācijas pakalpojuma prakses paziņojums un politika** pieejama [šeit](#)

<p>Dokumentu formātu un e-identifikācijas rīku dažādība</p>	<ul style="list-style-type: none"> • Dokobit atbalstītie dokumentu formāti: starptautiskie (PDF, ASiC-E) un Baltijas valstīs izmantotie (BDoc, EDoc and ADoc). • Dokobit darbojas ar dažādiem e-identifikācijas rīkiem, kurus izmanto visā Eiropā, sākot no ID kartēm līdz citiem e-identifikācijas rīkiem. Pilns atbalstīto e-identifikācijas rīku saraksts ir atrodams šeit 		
<p>Pozitīva lietotāju pieredze</p>	<ul style="list-style-type: none"> • Visi Dokobit e-parakstīšanās risinājumi ir balstīti uz Dokobit portālu, demonstrācija apskatāma šeit • Visi Dokobit risinājumi darbojas viedtālrunu pārlūkprogrammās • Dokobit portāls ir pieejams visiem iOS un Android lietotājiem, izmantojot mobilo lietotni 		
<p>Atbilstība uzņēmuma vajadzībām</p>	<p>Dokobit piedāvā:</p> <ul style="list-style-type: none"> • tiešsaistes portālu e-dokumentu parakstīšanai un parakstu vākšanai no trešajām pusēm. Pilns portāla funkciju saraksts ir pieejams šeit • jūsu pašu sistēmās integrējami risinājumi e-parakstīšanai, e-zīmogošanai, autentifikācijai. Plašāka informācija pieejama šeit 		
<p>Pakalpojumu sniedzēja reputācija</p>	<ul style="list-style-type: none"> • Dokobit uzticas dažādi uzņēmumi visā Eiropā, sākot ar finanšu sektoru un telekomunikācijām, beidzot ar automobiļu nozari un mazumtirdzniecību. Uzziniet vairāk no Dokobit klientiem šeit 		