ÚSTAVNÍ SOUD

JOŠTOVA 8, 660 83 BRNO

Vážený pan
…

V Brně dne 26. října 2021
Č. j.: SPR. ÚS 935/21-3 INF

Vážený pane,

na základě Vaší žádosti o informace podané dne 11. října 2021 dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „ZSPI“) Vám k Vaší první otázce sděluji, že informace zveřejňované Ústavním soudem v souladu se ZSPI jsou veřejnosti volně přístupné na stránkách https://www.usoud.cz bez omezení. K prohlížení webových stránek Ústavního soudu lze použít více internetových prohlížečů a volba prohlížeče je věcí každého jednotlivého držitele počítače (či jiného zařízení, na kterém je prohlížeč nainstalován). V průběhu jeho instalace musí každý uživatel souhlasit s licenčními podmínkami výrobce. V těchto licenčních podmínkách naleznete i Vy odpovědi na Vaše otázky, dotýkající se Vámi používaného bezpečnostního protokolu. Bezpečnostní protokol tedy závisí na Vašem prostředí a funkcích, které používáte. Ústavní soud Vám jakkoliv nemůže podat informaci o záležitostech, které jsou mezi Vámi a třetí stranou.

Pouze obecně Vám mohu sdělit, že bezpečnostní protokol TLS 1.2 je protokol určený k zajištění zabezpečení dat při přenosu přes síť. Důvody k vyřazení starších protokolů TLS 1.0 a TLS 1.1 spočívají v jejich zranitelnosti, neboť starší bezpečnostní protokoly nemohou zaručit adekvátní kybernetikou bezpečnost. V této souvislosti lze zmínit i fakt, že dne 11. října 2021 bylo Národním úřadem pro kybernetickou bezpečnost (dále jen „NÚKIB) vydáno ochranné opatření pro zabezpečení e-mailů, v němž NÚKIB přímo zavazuje Ústavní soud i další orgány veřejné moci k nutnosti pro elektronickou komunikaci prostřednictvím e-mailu používat bezpečnostní protokol minimálně TLS 1.2 (https://www.nukib.cz/cs/infoservis/aktuality/1758-spravci-klicovych-systemu-musi-zabezpecit-sve-e-mailove-schranky/).

K Vašemu druhému dotazu Vám sděluji, že i časové období změny bezpečnostních protokolů záleží na Vámi zvoleném webovém prohlížeči. Společnost Google díky svému prohlížeči Chrome ukončila podporu starších TLS protokolů verze 1.0 a 1.1 v roce 2020 s verzí Chrome 81. Ostatní poskytovatelé softwarových nástrojů pro prohlížení webových stránek jako např. Apple, Microsoft, Mozilla a jiní také postupně ukončují podporu starších bezpečnostních protokolů TLS 1.0 a 1.1.

Tím považuji Vaši žádost za vyřízenou.

JUDr. Vlastimil Göttinger, Ph.D.
generální sekretář Ústavního soudu

Tel.: 542 16 2111, fax: 542 16 1309
podani@usoud.cz