مطالعه تطبیقی تعهدات نهاد متقاضی پردازش، کنترلگر و پردازشگر تحت مقررات اروپایی حمایت از داده‌های شخصی و لایحه صیانت و حفاظت از داده‌های شخصی

حسن بادینی*
حمزه کرمی**

تاریخ دریافت: ۹۸/۰۴/۱۲ تاریخ پذیرش: ۹۸/۱۲/۰۶

چکیده

در بسیاری از مواقع نهادهایی که داده‌های افراد را به طور بالفعل یا بالقوه در اختیار دارند، اقدام به واگذاری پردازش داده ها به اشخاص ثالث می کنند، سوالی که مطرح می‌شود، این است که واگذاری پردازش به چه نوع ارائه دهندهٔ خدماتی می تواند به حفظ حریم خصوصی داده ها کمک کند؟ جای خالی پرداختن به تعریف و تعهدات نهاد متقاضی پردازش در GDPR و لایحهٔ صیانت و حفاظت از داده‌های شخصی احساس می‌شود. نهاد متقاضی علاوه بر اینکه باید بر تعهدات اولیهٔ خود آگاه باشد، لازم است تفاوت مسئولیت‌ها و تعهدات بین استفاده از کنترلگر و پردازشگر را نیز درک کند. بررسی تطبیقی این نقش‌ها تحت GDPR و لایحه بسیار کاربردی است، در خصوص تنقیح تکالیف کنترلگران و پردازشگران لایحه نیاز به اصلاحاتی دارد، اما در کل تحت هر دو مقرره واگذاری خدمات به یک کنترلگر مستقل برای حفظ حریم خصوصی افراد و کاستن از تعهدات نهاد متقاضی موثرتر است.

کلیدواژگان:
پردازشگر، کنترلگر، نهاد متقاضی پردازش.

---

* دانشیار دانشکده حقوق و علوم سیاسی، دانشگاه تهران
hbadini@ut.ac.ir

** دانش‌آموختهٔ دکتری حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه خوارزمی(نویسنده مسئول)
hamze.karami1@gmail.com

مقدمه

هر حرکتی در دنیای الکترونیک امروز از خود دنبالچهٔ اطلاعاتی بر جا می‌گذارد؛[۱] سازمان یا فروشگاهی که از خدمات معمولی امروزین چون کارت‌های الکترونیک یا برنامه‌های هوشمند بهره می‌برد، یا وسایل هوشمندی که از اینترنت اشیا بهره می‌گیرند،[۲] می‌توانند اقدام به جمع‌آوری داده‌های شخصی کارکنان یا مشتریان یا حتی اشخاص ثالث نمایند.[۳] به این ترتیب، این خطر وجود دارد که از این اطلاعات سوءاستفاده شود. بنابراین، باید در به‌کارگیری چنین محصولات و خدماتی مراقبت شود و به خطرات و تعهدات مربوط به حفظ حریم خصوصی و امنیت داده‌ها اشراف وجود داشته باشد. هدف اصلی از این تحقیق تدوین تعهداتی است که می‌تواند به مسئولیت کسانی که تصمیم به پردازش داده‌های دیگران می‌گیرند، بینجامد. این تصمیم ممکن است شخصاً یا با استخدام شخص‌ثالث عملی شود؛ تمرکز ما در این مطالعه بیشتر بر روی استخدام ارائه‌دهندهٔ شخص‌ثالث است. این نخستین تحقیق در ایران است که می‌خواهد ضرورت تدوین مسئولیت مذکور را مورد مطالعه قرار دهد؛ مسئله‌ای که حتی مورد غفلت قوانین روزآمد نیز قرار گرفته است و اگر بعد از تعلل زیاد برای تصویب قانونی جامع در حمایت از داده‌ها، این مسئله در لایحهٔ صیانت و حفاظت از داده‌ها مورد توجه قرار گیرد و مسئولیت‌های نهاد متقاضی پردازش داده به طور صریح ذکر گردد، می‌تواند به عنوان اولین قانون دنیا در این راستا قلمداد شود و به مثابه گامی بزرگ در راستای حفظ حقوق عامه مورد توجه و تحسین قرار گیرد. در راستای دستیابی به هدف مذکور، با توجه به محیط مطالعاتی، ابتدا مسئولیت‌ها، تعهدات ضمنی و فرض‌هایی را که در انواع قرارداد می‌تواند نشان‌دهندهٔ جایگاه نهاد متقاضی پردازش باشد، واکاوی می‌نماییم. در نهایت تفاوت تکالیف و الزامات کنترلگرها و پردازشگرها تحت GDPR و لایحهٔ صیانت و حفاظت از داده‌های شخصی مورد کنکاش قرار می‌گیرد. با مقایسهٔ لایحه با

۱. قاجار قیونلو، سیامک، مقدمه حقوق سایبر، تهران: میزان، ۱۳۹۱، ص ۳۴۳.

2. Daecher A, Cotteleer M, Holdowsky. J."The Internet of Things: A technical primer". 2018, available at: https://www2.deloitte.com/insights/us/en/focus/internet-of-things/technical-primer.html?icid=dcom_promo_featured|us;en (last visited on 25/012/ 2018)p5.

3. See:Stanescu, C. G. and Ievchuk, N, Alexa, Where Is My Private Data? Unanswered Legal and Ethical Questions Regarding Protection and Sharing of Private Data Collected and Stored by Virtual Private Assistants (May 3, 2018). Available at SSRN: https://ssrn.com/abstract=3250669(last visited on 17/08/ 2019).

استانداردهای GDPR نقاط قوت و ضعف آن را آشکار می‌نماییم. لازم به ذکر است، به دلیل اینکه بسیاری از اصول و تعهدات GDPR در سایر قوانین حریم‌خصوصی در سراسر جهان منعکس شده‌اند، بسیاری از نتایج می‌تواند نشان‌دهندهٔ مقایسه با استانداردهای روز دنیا باشد.[1]

سؤالات فرعی ما عبارت‌اند از اینکه تحت دو متن مورد مطالعه مسئولیت نهادی که اقدام به واگذاری پردازش به ارائه‌دهندهٔ ثالث می‌کند، چگونه است؟ و در چه صورتی نهاد متقاضی پردازش می‌تواند از دامنهٔ تعهدات خود بکاهد؟ سؤال اصلی نیز این است که واگذاری پردازش به چه نوع ارائه‌دهندهٔ خدماتی می‌تواند به حفظ حریم خصوصی داده‌ها کمک کند؟ فرضیهٔ ما می‌گوید: نهاد متقاضی مسئول قصور احتمالی در واگذاری چرخهٔ پردازش به افراد غیرصالح است. واگذاری پردازش به ارائه‌کننده‌ای که مانع تسلط نهاد متقاضی بر داده‌ها شود و مسئولیت کامل پردازش را برعهده بگیرد، می‌تواند هم به صیانت از داده‌ها کمک نماید و هم از دامنهٔ مسئولیت نهاد متقاضی بکاهد. در این مقاله از اصطلاحات اختصاری GDPR، لایحه و نهاد متقاضی، برای اشاره به دو متن مورد تطبیق و نهاد متقاضی پردازش استفاده می‌نماییم.

۱. تعهدات نهاد متقاضی

تعهدات نهاد متقاضی را می‌توان به دو دستهٔ کلی تقسیم نمود: گروهی از این تعهدات قبل از انعقاد قرارداد، تکالیفی‌اند که به موجب عرف یا قانون بر عهدهٔ نهادی که داده‌ها را در اختیار دارد، گذاشته شده‌اند؛ ما این تعهدات را تعهدات اولیهٔ نهاد متقاضی می‌نامیم؛ گروه دوم تعهداتی است که با واگذاری پردازش یا انجام پردازش ممکن است بدان متعهد شود، در حالی‌که امکان دارد در عمل حتی از آن اطلاعی نداشته باشد.

۱.۱. تعهدات اولیه متقاضی

نهاد متقاضی یک تعهد اولیه مبنی بر دقت در انتخاب شخص ارائه‌دهندهٔ خدمات به عنوان کنترلگر یا پردازشگر و اطمینان از اعتبار طرف قرارداد دارد. مطابق GDPR، صرف‌نظر از این‌که ارائه‌دهندهٔ ثالث پردازشگر یا کنترلگر باشد، نهاد متقاضی باید اقدامات معقولی را برای تعیین

1. Layton, R," How the GDPR Compares to Best Practices for Privacy, Accountability and Trust" (March 31, 2017). Available at SSRN: https://ssrn.com/abstract=2944358 or http://dx.doi.org/10.2139/ssrn.2944358(last visited on 20/12/ 2018)p1.

خط‌مشی‌ها و شیوه‌های حفاظت از داده‌ها توسط ارائه‌دهنده انجام دهد. همچنین باید اطمینان کامل یابد که ارائه‌دهندهٔ خدمات از داده‌هایی که جمع‌آوری می‌کند، به نحو شایسته‌ای محافظت می‌کند و از داده‌ها تنها برای مقاصد مشروع و متناسب استفاده خواهد نمود.[۱] انجام این تعهد، مستلزم آن است که نهاد متقاضی بررسی‌های لازم را انجام دهد و چنانچه امکان اعمال استانداردهای بالاتر وجود داشته باشد، بعید نیست عرف نهاد متقاضی را مکلف به آن نماید. هنگام استفاده از یک محصول یا سرویس ارائه‌شده توسط پردازشگر، نهاد تحت تعهد GDPR متعهد است «فقط از پردازشگرهایی که تضمین‌های کافی برای اجرای اقدامات فنی و سازمانی مناسب را ارائه می‌دهند، استفاده نماید؛ به گونه‌ای که پردازش با الزامات GDPR و اطمینان از حفاظت از حقوق افراد موضوع داده را تضمین می‌کند».[۲] شبیه این مقرره نیز در لایحه آمده است.[۳] شاید بتوان گفت این مسئولیت باید با استانداردهای سخت‌گیرانه‌تری اعمال شود؛ چرا که افراد موضوع داده برای دریافت خدمات یا امور کاری، بالاجبار اطلاعات خود را در اختیار آن نهاد گذاشته و در واقع اختیاری برای انتخاب گزینه‌های دیگر و احتیاط بیشتر در مقابل افراد موضوع داده وجود نداشته است. هر چند در صورت اختیار نیز عرف و قانون، دارندهٔ داده را مکلف به مواظبت و احتیاط در حد استاندارد می‌نماید. نهاد متقاضی پردازش را می‌توان امین قانونی افراد موضوع داده نیز دانست و او را مکلف به رعایت تعهدات قانونی و عرفی امین[۴] در قبال نگهداری و استفاده و انتقال داده‌ها دانست. در این راستا می‌توانیم از نظریهٔ مال‌انگاری داده‌ها که دست‌کم در قسمتی از داده‌ها که مشمول حق حریم خصوصی به معنای خاص می‌شوند و مورد پذیرش قرار گرفته است،[۵] استفاده نماییم و در قبال آن قسمت که از وصف مالیت خارج است و غالباً در قسمت حکمی حریم خصوصی قرار می‌گیرد که مربوط به حیثیت معنوی انسان است، می‌توانیم به

۱. به عنوان مثال، کار گروه ماده ۲۹ اعلام کرده است که در انتخاب یک دستگاه برای ارائه به کارکنان، جایی که دستگاه اطلاعات مربوط به تناسب اندام را به کنترلگر شخص ثالث ردیابی و ارسال می کند، کارفرما باید سیاست حفظ حریم خصوصی سازنده و یا ارائه دهنده خدمات را به منظور اطمینان از اینکه به پردازش غیرقانونی اطلاعات بهداشتی در مورد کارکنان منجر نخواهد شد، بررسی نماید. (کارگروه ماده ۲۹ حفاظت از داده ها، نظر ۲۰۱۷/۲ در مورد پردازش داده‌ها در محل کار (WP249)، در تاریخ ۸ ژوئن ۲۰۱۷).

۲. بند۱ماده ۲۸.

۳. ماده ۲۰.

۴. باقری، احمد و مریم حجتی، بررسی تعهدات امین در فقه امامیه و حقوق موضوعه، پژوهش‌های فقهی، زمستان ۱۳۹۳، شماره ۴، ص ۶۷۱.

۵. قنواتی، جلیل و حسین جاور، حریم خصوصی؛ حق یا حکم، مجله حقوق اسلامی، زمستان ۱۳۹۰، شماره ۳۱، ص۲۷.

منابع تعهد دیگر، از جمله اصول متعدد در پردازش، مثل اصل امنیت و عدم انتقال یا تعهدات اخلاقی و عرفی چون لزوم رازداری و احتراز از افشای اسرار و حتی مفهوم اصل اباحه،[1] استناد نماییم.

دیگر تعهد اولیه و ضمنی نهاد متقاضی را می‌توان در الزام او به انعقاد قرارداد با ارائه‌دهندهٔ خدمت، اعم از کنترلگر و پردازشگر، دانست که البته در GDPR این الزام فقط ضمنی نیست، بلکه در جاهایی شکل تکلیف قانونی به خود می‌گیرد؛ از جمله آنچه در بند ۱۰۹ دیباچه GDPR آمده است. انعقاد قرارداد به دلایل ذیل حائز اهمیت است: ایجاد درک صریح و روشن طرفین قرارداد، خصوصاً کنترلگر و پردازشگر از وظایف و مسئولیت‌های خود، رعایت مؤثرتر قواعد و الزامات مندرج در قوانین و مقررات حمایت از داده، ارتقای سطح کنترل و حفاظت از اطلاعات شخصی، رسمیت بخشیدن به روابط کاری کنترلگر و پردازشگر. همچنین قرارداد یا توافق بین نهاد متقاضی و ارائه‌دهنده می‌تواند یک منبع مهم تعهدات حفاظت از داده‌ها باشد. این قرارداد می‌تواند وسیلهٔ تعیین و محدود کردن حدود جمع‌آوری و استفاده از داده‌ها، تخصیص نقش‌ها و مسئولیت‌ها، و الزام طرفین به اقدامات حفاظت از داده باشد. تعهدات قانونی بسته به اینکه ارائه‌دهنده پردازشگر یا کنترلگر باشد، به طور قابل توجهی متفاوت است. اما در عمل، نهاد متقاضی می‌تواند تعهدات قوی‌تری را از ارائه‌دهنده در قرارداد بگیرد و تفاوت عملی بین کنترلگر و پردازشگر در این خصوص وجود ندارد.

عنوان قرارداد در تعیین وضعیت واقعی آن تعیین‌کننده نیست و باید این تعیین بر اساس شرایط بیرونی و واقعی باشد.[2] در گفتارهای بعدی ضمن بر شمردن تکالیف قانونی هر یک از کنترلگران و پردازشگران که طرف قرارداد نهاد متقاضی‌اند، مواردی نیز که لازم است یا مطلوب‌تر است در قرارداد ذکر شود، به فراخور بیان می‌گردد.

۱.۲. تعهدات قراردادی یا عملی نهاد متقاضی

اقدام به پردازش یا بهره‌گیری از خدمات پردازش بر روی داده‌های دیگران دارای تبعات حقوقی معتنابهی می‌باشد. یک باور عمومی رایج این است که در چنین شرایطی، نهاد متقاضی کنترلگر و ارائه‌دهندهٔ خدمات، پردازشگر قلمداد شود. اما چنین قاعده‌ای تمامی موارد را شامل

۱. فروغی، فضل الله، محمدناصر برجی و جواد مصلحی، مبانی ممنوعیت نقض حریم خصوصی در حقوق ایران و آمریکا، مطالعات حقوقی، پاییز ۱۳۹۳، شماره ۳، ص۱۴۷.

2. Article 29 Data Protection Working Party, 2010, 9.

نمی‌شود و موارد متعددی وجود دارد که خارج از فرض مذکور است. برای عملیات پردازش داده‌های شخصی در اختیار نهاد متقاضی چهار فرض متصور است:

۱. نهاد متقاضی از خدمات یک پردازشگر استفاده نماید.

۲. نهاد متقاضی از خدمات یک کنترلگر مستقل استفاده نماید و خود نیز در امر کنترلگری دخالت ننماید.

۳. نهاد متقاضی از خدمات یک کنترلگر مشترک استفاده نماید.

۴. نهاد متقاضی بدون دریافت خدمات از ارائه‌دهندهٔ خدمت خود اقدام به پردازش داده‌ها نماید.

در فرض اول، نهاد متقاضی دارای نقش و مسئولیت‌های یک کنترلگر است. ولی در فرض دوم نهاد متقاضی دارای عنوان قانونی مذکور در GDPR و لایحه نیست. ما در این فرض از او به عنوان کارفرما یاد می‌کنیم، کارفرما کسی است که دیگری را اجیر کند تا به دستور وی کاری معین را انجام دهد.[۱] اما در فرض سوم نهاد متقاضی کنترلگر مشترک محسوب می‌شود و به همراه کنترلگر ارائه‌دهندهٔ خدمات دارای نقش‌های کنترلگری است و از نظر مسئولیت همان کنترلگر مستقل محسوب می‌شود.[۲] در فرض آخر مسئولیت پردازشگر و کنترلگر هر دو متوجه نهاد پردازش‌کننده است.

۲. بررسی وظایف قانونی خاص و ملاحظات مربوط به پردازشگر و کنترلگر تحتGDPR و لایحه

با توجه به اینکه نهاد متقاضی پردازش ممکن است با اتخاذ هر کدام از رویه‌های فوق‌الاشعار مسئولیت‌های کنترلگری یا پردازشگری را به طرف مقابل بسپارد یا خود مستقلاً یا مشترکاً عهده‌دار برخی از این مسئولیت‌ها شود، لذا لازم است مسئولیت‌های این دو عنصر را به طور کلی، همچنین در برخی موارد شاخص به صورت موردی، تطبیق و بررسی نماییم.

۲.۱. قرارداد با پردازشگر، وظایف قانونی خاص و ملاحظات مربوطه تحت GDPR

قرارداد بین نهاد متقاضی و پردازشگر باید شامل تمام موارد مذکور در مادهٔ ۲۸ GDPR باشد و همچنین باید برخی از الزامات دیگر GDPR را منعکس کند؛ از جمله ماهیت، هدف و موضوع

۱. جعفری لنگرودی، محمد جعفر، مبسوط در ترمینولوژی حقوق، تهران: گنج دانش، ۱۳۸۷، ص ۲۹۸.
۲. بند ۱ و ۳ ماده ۲۶ GDPR.

پردازش انوع داده‌های شخصی، مدت زمان پردازش و تعهدات و حقوق نهاد متقاضی. بـه عـلاوه بند ۳ مادۀ ۲۸ چند مورد خاص را برای گنجاندن در قرارداد با یک پردازشگر، تصریح می‌کند کـه پردازشگر: پردازش اطلاعات شخصی را فقط براساس دستورالعمل‌های مستند نهاد متقاضی و بـا اطلاع قبلی انجام دهد. در صورت نیاز پردازشگر به پردازش داده‌ها تحت قانون کشور عضو بایـد به اطلاع شخص موضوع داده برسد. (مگر اینکه چنین اطلاعی توسـط قـانون منـع شـده باشـد) همچنین پردازشگر باید تضمین کند که اشخاص مجاز برای پردازش، متعهد به محرمانگی داده‌ها هستند و اتخاذ تمام اقدامات امنیتی مورد نیاز در ماده ۳۲ نیز ضروری است.

اگر پردازشگر، پردازشگر دیگری را وارد پردازش کند،[۱] تمامی تعهدات، مندرج در قـرارداد یـا دیگر توافقات قانونی، بین نهاد متقاضی و پردازشگر، باید به پردازشگرهای بعدی منتقل شود؛ بـه خصوص این پردازشگرها باید تضمین کافی برای پیاده‌سازی معیارهای فنی و سازمانی مناسب را برای رفع تمامی الزامات مقررات GDPR ارائه دهند. زمانی که دیگـر پردازشـگرها قـادر نباشـند تعهدات حفاظت داده را برآورده سازند، پردازشگر اولیـه مسـئول پاسـخگویی نسـبت بـه عملکـرد ضعیف دیگر پردازشگرها خواهد بود.[۲] با توجه به ماهیت پردازش، پردازشگر باید تا آنجا که ممکن است، با استفاده از معیارهای فنی و سازمانی مناسب، در انجام تعهد نسـبت بـه پاسـخ‌گـویی بـه درخواست‌های مربوط به حقوق شخص موضوع داده که در فصل سوم GDPR مطرح شده است، به نهاد متقاضی کمک کند. همچنین در تضمین سازگاری با تعهدات مطرح شده در مادۀ ۳۲، بـا در نظر گرفتن ماهیت پردازش و اطلاعات قابل دسترس بـرای پردازشـگر، بـه نهـاد متقاضـی در تضمین انطباق با الزامات مربوط به امنیت داده‌ها، اطلاع نقض، ارزیابی تاثیر حفاظت از داده‌ها[۳] و مشاورۀ قبلی با مقامات نظارتی کمک نماید.[۴] همچون نهاد متقاضی، پردازشـگر نیـز موظـف بـه اتخاذ تدابیر لازم برای حفظ امنیت داده‌ها است. مطابق بند دوم مادۀ ۳۳، در صورت وقوع نقـض در داده‌ها، پردازشگر باید نهاد متقاضی را سریعاً مطلع نماید. هنگامی کـه خـدمات پردازشـگر بـه نهاد متقاضی مربوط به پردازش تکمیل می‌شوند، با درخواست او، پردازشگر موظف به بازگرداندن

۱. تنها با اجازه کتبی قبلی کنترلگر می‌تواند- بند ۳ ماده ۲۸ GDPR.
۲. بند ۴ماده ۲۸.
3. DPIAs
۴. پاراگراف f از بند ۳ ماده ۲۸.

همهٔ نسخه‌های داده‌های شخصی به نهاد متقاضی یا حذف آنهاست.[۱] پردازشگر باید تمام اطلاعات لازم را در اختیار نهاد متقاضی به منظور نشان دادن انطباق خود با الزامات حفاظت از داده‌ها به مرجع صالح قرار دهد و به حسابرسی یا بازرسی انجام‌شده توسط نهاد متقاضی یا کارشناس برگزیدهٔ او کمک کند.[۲] علاوه بر این، بخش‌های دیگر GDPR تعهدات دیگری را بر پردازشگرها تعیین می‌کند؛ به‌عنوان مثال، مطابق مادهٔ ۳۰، پردازشگرها باید جزئیات فعالیت‌های پردازش داده‌ها را مستند کنند. به همین ترتیب، نهاد متقاضی می‌تواند یک تعهد کلی را از پردازشگر به منظور تطبیق کامل فعالیت تحت قوانین حفاظت از داده‌های اخذ نماید. هر چند اگر قرارداد به‌طور کلی نیز بسته شود، پردازشگر ملزم به کمک به نهاد متقاضی در انجام تعهدات مربوطه می‌باشد، بهتر است این تعهدات در قرارداد با پردازشگر برای تضمین انطباق کامل منعکس شود.

۲.۲. قرارداد با پردازشگر، وظایف قانونی خاص و ملاحظات مربوطه تحت لایحه

لایحه در این فرض یا فرض‌های دیگر از لزوم عقد قرارداد سخنی به میان نیاورده است. اما می‌توان با توجه به تعهد عرفی و قانونی نهاد متقاضی، او را موظف دانست که در راستای رعایت حقوق افراد موضوع داده و مشخص شدن تکالیف و گرفتن تضمین‌های لازم با پردازشگر، قرارداد منعقد نماید. لایحه، پرداشگر را صرفاً در شرایطی که تأکید خاص قانونی یا قراردادی در راستای مسئولیت وی باشد، مسئول می‌داند.[۳] با توجه به مادهٔ ۱۵، مادهٔ ۱۸ لایحه نیز حمل بر تعدد هر یک از کنترلگران یا پردازشگران با هم نوع خودشان می‌شود. لایحه در موارد متعددی به تکالیف قانونی پردازشگر اشاره می‌کند که نیاز به تکرار در قرارداد ندارند، ولی چنانچه از باب تأکید ذکر شود، مفید می‌باشد؛ از جمله اینکه، پردازشگر باید تجهیزات و نیروی انسانی مورد نیاز برای حسن ایفای تعهدات نظارت‌پذیری پردازش بر خودش را فراهم آورد،[۴] تاکید بر اطلاع‌رسانی،[۵] تعهدات

۱. پاراگراف g از بند ۳، ماده ۲۸ .GDPR .

۲. ماده ۲۸ (۳) همچنین بیان می‌دارد: تمامی اطلاعات لازم برای ثابت کردن سازگاری با تعهدات این ماده را در اختیار کنترلگر قرار داده و امکان انجام حسابرسی و تفحص را برای کنترلگر یا نمایندگان مشخص شده توسط کنترلگر فراهم کند. با توجه به بند h (پاراگراف اول)، اگر پردازشگر تشخیص دهد که دستورالعملی با قانون حفاظت داده در اتحادیه یا کشورهای عضو سازگار نیست، باید سریع کنترلگر را مطلع سازد.

۳. ماده ۱۵

۴. ماده۲۴.

۵. ماده۲۶.

حفظ ایمنی،[۱] نگهداری داده‌ها،[۲] هزینهٔ اجرای دستورالعمل‌های حفاظتی و نیازمندی‌های نظارتی،[۳] مسئولیت مستقل،[۴] شرایط معافیت از مسئولیت.[۵] اما چنانچه طرفین مایل باشند دامنهٔ مسئولیت را تغییر دهند، باید حتماً در قرارداد ذکر شود؛ مثل اینکه بخواهند مسئولیت مندرج در مادهٔ ۶۱ را به نفع موضوع داده در مورد پردازشگر نیز برقرار سازند.

۲.۳. قرارداد با کنترلگر و وظایف قانونی خاص و ملاحظات مربوطه تحت GDPR

اگر نهاد متقاضی پردازش را به یک کنترلگر واگذار نماید و در امر کنترلگری هیچ دخالتی ننماید، کنترلگر مسئول عملیات پردازش می‌شود و باید قادر به نشان دادن سازگاری عملکردش با اصول مرتبط با پردازش داده‌های شخصی باشد.[۶] مطابق GDPR به شرایط قراردادی خاصی بین نهاد متقاضی که نقش یک کارفرما را دارد و ارائه‌دهنده نیاز نیست، اما می‌توان با توجه به تعهد عرفی و قانونی، نهاد متقاضی او را مکلف به انعقاد قرارداد به منظور رعایت حقوق افراد موضوع داده و مشخص شدن تکالیف و گرفتن تضمین‌های لازم دانست. در مواردی که کارفرما (نهاد متقاضی) داده‌ها را از اتحادیهٔ اروپا به کنترلگری در خارج از اتحادیه منتقل می‌کند، باید اطمینان حاصل کند کشور ثالث یا بخش و بخش‌هایی درون کشور ثالث، یا سازمان بین‌المللی دارای سطح قابل قبولی از حفاظت هستند[۷] و توصیه می‌شود در راستای منافع تجاری، کارفرما اطمینان حاصل کند که کنترلگر، تعهدات قراردادی را برای حفاظت از داده‌ها و استفاده از آن فقط برای مقاصد مشروع و مناسب مورد استفاده قرار دهد.

اما در صورتی‌که نهاد متقاضی در امر کنترلگری دخالت نماید، خود نیز کنترلگر مشترک محسوب می‌شود؛ لذا مسئولیت هر یک از کنترلگرها باید به طور شفاف، سازگار با تعهدات تحت پوشش GDPR مشخص شود؛ به ویژه نسبت به حقوق افراد موضوع داده و وظایف آنها برای

۱. ماده ۲۸.
۲. مواد۳۳ و۳۴.
۳. مواد۳۶و۵۷.
۴. ماده۵۹.
۵. ماده۶۰.
۶. بند۲ماده ۵.
۷. بند۱ماده۴۵.

فراهم کردن اطلاعات مرتبط با مواد سیزده[۱] و چهارده،[۲] با استفاده از وظایف محوله به هریک از آنها، مگر اینکه در آینده، مسئولیت کنترلگرها توسط قانون اتحادیه یا کشورهای عضو برای کنترلگرهای مشترک، تعیین شود؛ این ترتیب می‌تواند یک راه تماس برای شخص موضوع داده باشد. ترتیب اشاره شده باید به قدر لازم نقش‌ها و ارتباطات مربوط به کنترلگرهای مشترک را نسبت به افراد موردنظر مشخص نماید. ماهیت ترتیب باید در دسترس افراد موضوع داده قرار گیرد، شرایط قرارداد بین کنترلگرهای مشترک، در مقابل اشخاص موضوع داده قابلیت استناد ندارد و مشارالیهم می‌توانند حقوق خود را در رابطه با و در مقابل با هر یک از کنترلگرها به طور مستقیم و تضامناً استیفا نمایند.[۳] در زمانی که نوعی از پردازش با استفاده از فناوری‌های جدید، با در نظر گرفتن ماهیت، قلمرو، موضوع و اهداف پردازش، منجر به ریسک بالا برای حقوق و آزادی‌های اشخاص حقیقی شود، کنترلگر باید پیش از انجام پردازش، ارزیابی اثرات عملیات پردازشی پیش‌بینی شده را با هدف حفاظت از داده‌های شخصی، در نظر داشته باشد[۴] و در شرایط خاص با نهاد نظارتی مشاوره نماید.[۵]

به علاوه در مادۀ ۲۴ gdpr تعهداتی خاص کنترلگر در نظر گرفته شده است که عبارت‌اند از: ۱) با توجه به ماهیت، قلمرو، موضوع و اهداف پردازش و همچنین ریسک‌های متنوع از نظر احتمال و شدت برای حقوق و آزادی‌های فردی، کنترلگر باید معیارهای فنی و سازمانی مناسبی را برای تضمین و اثبات تطابق پردازش با این قوانین را پیاده‌سازی کند. هر زمان که لازم باشد این معیارها، باید بازبینی و به‌روزرسانی شوند. ۲) در موارد متناسب با فعالیت‌های پردازش، اقدامات ذکر شده در بند ۱ شامل اجرای سیاست‌های مناسب برای حفاظت از داده توسط کنترلگر می‌باشد. ۳) پایبندی به کدهای اجرایی تأییدشده اشاره شده در مادۀ ۴۰، یا مکانیزم‌های گواهی تأییدشده اشاره شده در مادۀ ۴۲، می‌تواند به عنوان عنصری استفاده شود که سازگاری با تعهدات و الزامات کنترلگر را ثابت کند. مطابق مادۀ ۲۵ مقررات مربوط به حفاظت از داده با استفاده از طراحی و به طور پیش‌فرض نیز از تعهدات کنترلگر است.

۱. اطلاعاتی که باید بعد از جمع‌آوری داده‌های شخصی از شخص موضوع داده ارائه شوند.
۲. اطلاعاتی که به هنگام عدم دسترسی شخص موضوع داده، به داده‌های شخصی، ارائه می‌شوند.
۳. بند ۳ ماده ۲۶.

4. Data protection impact assessment.

۵. مواد ۳۵ و ۳۶.

۲.۴. قرارداد با کنترلگر و وظایف قانونی خاص و ملاحظات مربوطه تحت لایحه

لایحه در فرض واگذاری خدمات به کنترلگر نیز از لزوم عقد قرارداد بین نهاد متقاضی و کنترلگر سخنی به میان نیاورده است، در اینجا نیز با توجه به تعهد عرفی و قانونی نهاد متقاضی، می‌توان او را موظف دانست با کنترلگر قرارداد منعقد نماید. موارد مسئولیت کنترلگر تحت لایحه به طور کلی فراگیر و در تمام مراحل برقرار است.[۱] برخی از تعهدات عملیات پردازش ویژه و خاص کنترلگر است؛ همچون در خواست توقف پردازش که از کنترلگر به عمل می‌آید و او باید سازوکار دریافت این درخواست و انتقال به پردازشگر را فراهم سازد.[۲] اصل بر تعهد کلی کنترلگر است،[۳] در صورت تعدد، مسئولیت کنترلگران در رابطه بین خودشان برابر است.[۴] فراهم آوردن همهٔ امکانات، تجهیزات و نیروی انسانی در راستای نظارت‌پذیری پردازش، در امور کنترلگری به عهدهٔ کنترلگر است و[۵] پاسخگویی کامل دربرابر اشخاص موضوع داده[۶] و تکلیف کلی بر جبران خسارت.[۷] اما در بخش دیگری از تعهدات و مسئولیت‌های مربوط به عملیات پردازشی تفاوتی بین پردازشگر و کنترلگر وجود ندارد و هر دو مسئولیت دارند. این تعهدات عبارت‌اند از: تعهد بر اطلاع‌رسانی،[۸] تعهدات حفظ ایمنی،[۹] نگهداری داده‌ها،[۱۰] هزینهٔ اجرای دستورالعمل‌های حفاظتی و نیازمندی‌های نظارتی،[۱۱] مسئولیت مستقل هر دو در برابر تعهدات مربوط به خودشان.[۱۲]

۱. مواد ۳۱ و ۳۲.
۲. ماده ۸.
۳. ماده ۱۵.
۴. ماده ۱۸.
۵. ماده ۲۴.
۶. مواد ۳۱ و ۳۲.
۷. ماده ۶۱.
۸. ماده ۲۶.
۹. ماده ۲۸.
۱۰. مواد ۳۳ و۳۴.
۱۱. ماده ۳۶ و ۵۷.
۱۲. ماده ۵۹.

۳. بررسی موردی برخی تعهدات خاص و مهم

برای سنجیدن دقیق‌تر عیار این دو سند، لازم است بعد از بررسی برخی از اصول مهم اظهار نظر نماییم:

۱.۳. اصل شفافیت (اطلاع)

اصل شفافیت با اصل اطلاع تفاوت قابل ذکری ندارد و برخی محققان نیز که این دو را از هم تفکیک نموده‌اند، اصل شفافیت را اطلاع‌رسانی به شخص موضوع داده یا مقام‌های ناظر دانسته‌اند؛[۱] لذا ما این دو را مترادف می‌دانیم و بر تفکیک این دو، حتی بر فرضی که بتوان نقطهٔ افتراقی برای آنها یافت، اثری مترتب نمی‌دانیم. این اصل از حق دانستن که یکی از حقوق بنیادین انسان است، سرچشمه می‌گیرد. اصل دانستن و حق بر آگاهی انسان‌ها این فرض مهم را در خود دارد که آدمیان اساساً موجوداتی خردورز و دارای قوهٔ داوری و قادر به تشخیص صلاح خویشتن‌اند. بر این اساس، هرگونه رفتار قیم‌مآبانه نافی این اصل بنیادین است.[۲] برای حصول اطمینان از روند پردازش شفاف و عادلانه، داده‌ها باید برای اهداف مشخص، صریح و قانونی جمع‌آوری شوند. جمع‌آوری داده‌ها بایستی به اطلاع شخص موضوع داده برسد و ضمن آن اطلاعاتی که در رضایت یا عدم رضایت وی مؤثر است، به آگاهی وی برسد؛ همچنین اگر قانونی برای الزام به پردازش وجود دارد و نیز نتیجهٔ عدمِ رضایت به شخص موضوع داده‌ها اطلاع داده شود. در مادهٔ ۵۹ قانون تجارت الکترونیک و در بیان شرایط پردازش مواردی آمده است که از برخی از آنها می‌توان اصل شفافیت را برداشت نمود؛ از جمله اینکه اهداف پردازش باید مشخص بوده و به طور واضح شرح داده شده باشد و شخص موضوع «داده پیام» باید به پرونده‌های رایانه‌ای حاوی «داده پیام»های‌شخصی مربوط به خود دسترسی داشته باشد.

۳.۱.۱. شفافیت تحت GDPR

مطابق GDPR لازم است که حقوق افراد موضوع داده با مجموعهٔ جامعی از اطلاعات مربوط به مسئولیت‌های کنترلگر، جزئیات داده‌های شخصی جمع‌آوری‌شده و پردازش آن، آشنایی

۱. اصلانی، حمیدرضا. حقوق فناوری اطلاعات، تهران: میزان. ۱۳۸۹.ص ۱۳۹.
۲. پدرام، سعید و حمیدرضا رحمانی‌زاده دهکردی، شفاف‌سازی و پاسخگویی در نهادهای رسمی. نشریه مجلس و راهبرد، زمستان ۱۳۸۱، شماره ۳۶ : ۸۵-۹۵، ص ۸۷.

با حقوق خود و چندین موضوع دیگر رعایت شود.[۱] کنترلگر باید معیارهای مناسبی را برای فراهم کردن اطلاعات مندرج در مواد ۱۳ و ۱۴ و هرگونه مخابرهٔ آنها تحت مواد ۱۵ تا ۲۲ و مادهٔ ۳۴ که مربوط به دسترسی شخص موضوع داده، به صورت شفاف، هوشمندانه و قابل دسترس با استفاده از زبانی قابل فهم، در نظر گیرد.[۲] اطلاعاتی که باید به موضوع داده رسانده شود، بسیار گسترده‌تر از آنچه در قانون قبلی حفاظت از دادهٔ اتحادیه اروپا آمده بود، است و معمولاً در کل یا بخشی از آن، از طریق یک بیانیهٔ محرمانهٔ شخصی یا اخطاریهٔ حریم‌خصوصی ارائه می‌شود.[۳] همچنین زمانی که در زمینهٔ داده‌های شخصی نقضی ایجادشده باشد، کنترلگر باید بدون تأخیر و حداکثر ظرف ۷۲ ساعت بعد از آگاهی از این امر، بر اساس مادهٔ ۵۵، نهاد نظارتی را مطلع سازد؛ مگر اینکه بعید باشد نقض دادهٔ حقوق و آزادی‌های فردی را تهدید نماید. اگر اعلام به نهاد نظارتی ظرف ۷۲ ساعت انجام نشود، باید دلایل تأخیر نیز ارسال شود[۴] و زمانی‌که نقض داده‌های شخصی به احتمال زیاد منجر به ریسک بالا برای حقوق و آزادی‌های اشخاص حقیقی شود، کنترلگر باید بدون تأخیر، با شخص موضوع داده نیز مکاتبه کند.[۵] این تعهدات مستقیماً و فقط بر عهدهٔ کنترلگر گذارده شده است. با این حال، اگر پردازشگر از یک نقض اطلاعات شخصی مطلع شود، باید کنترلگر را مطلع سازد.[۶] همچنین پردازشگر یک تعهد برای کمک به کنترلگر در برآورده کردن الزامات هشدار کنترلگر دارد.[۷] علاوه بر این، به نظر نمی‌رسد که هیچ ممنوعیتی برای محول کردن تکلیف اطلاع‌رسانی به پردازشگر وجود داشته باشد و کنترلگر می‌تواند در قرارداد با پردازشگر این تکلیف را به او محول نماید. البته این مقرره در مقابل افراد موضوع داده قابل استناد نمی‌باشد. بنابراین، اگر نهاد متقاضی پردازش از خدمات یک پردازشگر استفاده نماید، قاعدتاً خود او کنترلگر به حساب می‌آید و باید در ساختار خود یک فرایند واکنش موردی را

۱. مواد۱۳، ۱۴ و بندهای ۱و۲، ماده ۱۵.
۲. ماده ۱۲.
3. Hintze M," In Defense of the Long Privacy Statement". Maryland Law Review. 76 .1044. 2017.
۴. ماده ۳۳ بند ۱.
۵. ماده ۳۴بند ۱.
۶. ماده ۳۳بند ۲.
۷. ماده ۲۸ بند۳.

پیش‌بینی نماید تا در جایی که هشدار را از سوی پردازشگر دریافت می‌کند،[۱] بتواند آن را به افـراد موضوع داده و نهاد نظارتی برساند.[۲] به همین ترتیب، اگر نهاد متقاضی و ارائه‌دهنده، کنترلگرهای مشترک باشند، باید هر کدام فرایندهای مشابه و خاص خود را داخل تشکیلات خود داشته باشند و یک ترتیب بین آنها برای مشخص کردن مسئولیت هر یک از طـرفین بـرای اطـلاع دادن بـه افراد موضوع داده وجود داشته باشد.[۳] اگر ارائه‌دهنده یک کنترلگر مستقل باشد، تنها او مسـئولیت نظارتی برای پاسخگویی به هرگونه تخلف از داده ها در کنتـرل خـود و ارسـال اطلاعیـه خواهـد داشت و نهاد متقاضی در این موقعیت نقش قانونی مسئولیت‌آفرینی به‌جز تکالیف اولیه که قبلاً بر شمردیم، ندارد.

۳.۱.۲. شفافیت تحت لایحه

صرف‌نظر از انشای ضعیف مادۀ ۲۶ لایحۀ این مـاده بـر خـلاف GDPR هـر دو (یـا یکـی) کنترل‌گر (و) یا پردازشگر را موظف به اطلاع‌رسانی به شخص موضـوع داده دانسـته اسـت کـه اطلاعات ذیل را در اختیار یا در دسترس اشخاص موضوع داده قرار دهد: هدف پـردازش، نـوع و نحوۀ پردازش، هویت، ماهیت و فعالیت کنترلگران یا پردازشگران اصلی و مـرتبط؛ موقعیـت‌هـا و وضعیت‌های پردازش، اعم از عمومی و غیرعمومی؛ منابع پردازش، از قبیل پایگاه‌هـای اطلاعـات مؤسسات عمومی یا خصوصی یا برگزاری آمایش‌ها و پیمایش‌های گوناگون؛ ویژگی‌ها و شـرایط فنی پردازش، گواهی‌ها یا پروانه‌های دریافت شده از مراجع صلاحیت‌دار؛ سـطح ایمنـی و امنیـت پردازش و دانش و هزینۀ مترتب بر آن؛ حـق‌هـای اشـخاص موضـوع داده نسـبت بـه پـردازش داده‌های شخصیشان و چگونگی استیفای آنها؛ ناظر ویژۀ پـردازش و سـایر مراجـع صـلاحیت‌دار نظارتی و رسیدگی‌کننده به شکایات اشخاص موضوع داده. در لایحه، ظاهراً کنترلگر یا پردازشگر هیچ وظیفه‌ای مبنی بر اطلاع‌رسانی به افراد موضوع داده در زمان نقض ندارند. البته اگر بند «ح» ماده ۲۶ را به طور موسع و برخلاف ظاهر آن تفسیر نماییم و آن را در هـر مـوقعیتی کـه سـطح ایمنی و امنیت پردازش دچار تغییر شود، کنترلگر یا پردازشگر را موظف بدانیم کـه اطـلاع‌رسـانی

۱. بند ۲ ماده۳۳.
۲. بند ۱ ماده ۳۳ و بند ۱ ماده ۳۴.
۳. ماده۲۶.

نماید، وضعیت تغییر می‌کند و آنگاه سازوکار اطلاع‌رسانی نیز برخلاف GDPR صرفاً از طریق کنترلگر نیست.

۳.۲. امنیت داده به‌طور کلی

کسی که داده‌ها را در اختیار دارد، باید تلاش خود را تا حدود امکانات فنی متعارف در راستای جلوگیری از پردازش غیر مجاز داده‌ها به معنی اعم، توسط اشخاص غیرمجاز به‌کار گیرد. امنیت داده از جمله دغدغه‌های مهم در عصر پردازش ابری و کلان داده است.[۱] این اصل در تمامی مراحل نگهداری و به کارگیری و حتی امحای داده‌ها جاری است.[۲]

۳.۲.۱. امنیت داده‌ها[۳] تحت GDPR

الزامات امنیتی داده در مادهٔ ۳۲ گنجانده شده‌است. این ماده در مورد کنترلگرها و پردازشگرها هر دو اعمال می‌شوند. هر دوی آنها ملزم به «اجرای اقدامات فنی و سازمانی مناسب برای تضمین سطح امنیت مناسب در مقابله با خطر می‌باشند».[۴] موارد خاص که ممکن است در چنین اقداماتی گنجانده شوند، در مادهٔ ۳۲ عبارت‌اند از: ۱- مستعارسازی و رمزنگاری داده‌های شخصی؛ ۲- توانایی تضمین محرمانگی، یکپارچگی، دسترس‌پذیری و مقاومت سامانه‌ها و خدمات پردازشی به طور مداوم؛ ۳- توانایی بازیابی دسترس‌پذیری و دسترسی به داده‌های شخصی به شکل زمان‌بندی شده، در هنگام وقوع حادثه فیزیکی یا فنی؛ ۴- فرایندی برای سنجش و ارزیابی منظم اثربخشی معیارهای فنی و سازمانی برای تضمین امنیت پردازش. بر اساس GDPR در هنگام ذخیره‌سازی، داده باید مستعارسازی[۵] و رمزنگاری[۶] شود.[۷]

---

۱. جان‌نثاری، اعظم، فاطمه ترابی و فاطمه علی نجیبی نیا، تحول عظیم ابرداده‌ها و بررسی چالش‌های آن، سومین کنفرانس بین المللی پژوهش در علوم و تکنولوژی، برلین آلمان، ۱۳۹۵، ص ۸.

2. See: Esayas, S.” The Role of Anonymisation and Pseudonymisation Under the EU Data Privacy Rules: Beyond the ‘All or Nothing”. European Journal of Law and Technology, Vol 6, No 2, 2015.

3. Data security

۴. ماده ۳۲، بند۱.

5. pseudonymisation

6. encryption

۷. ماده ۶ بند۴ پاراگراف e و ماده ۳۲ بند ۱ پاراگراف a. مستعارسازی یعنی پردازش داده‌های شخصی به نحوی که داده‌های شخصی بدون استفاده از سایر اطلاعات، قابلیت نسبت داده شدن به فرد خاص را نداشته باشند، این اطلاعات اضافی به صورت جداگانه نگهداری شده و تحت ارزیابی‌های فنی و سازمانی قرار می‌گیرند تا اطمینان حاصل شود که داده‌های شخصی به شخص حقیقی شناسایی شده یا قابل شناسایی، نسبت داده نشده است. (ماده ۴، بند۵)

علاوه بر این، کنترلگرها باید در قرارداد خود با پردازشگر الزام به رعایت این تعهدات نماید[1] و هر پردازشگری از طریق قرارداد با پردازشگری نیز که وارد عملیات پردازش می‌کند، باید این تعهدات را در نظر بگیرد. بنابراین، اینکه ارائه‌دهنده به عنوان یک کنترلگر یا یک پردازشگر عمل می‌کند، الزامات امنیتی مشابه اعمال می‌شوند. لذا با توجه به امنیت داده‌ها، تنها تفاوت این است که وقتی یک نهاد متقاضی از محصول یا خدمات ارائه شده توسط یک پردازشگر استفاده می‌کند، باید قراردادی برای انطباق با الزامات امنیتی مادۀ ۳۲ وجود داشته باشد؛ در حالی‌که در هنگام استفاده از خدمات ارائه شده توسط کنترلگر، انعقاد قرارداد الزام قانونی ندارد؛ با وجود این، علاوه بر تعهد عرفی و قانونی در قبال افراد موضوع داده، منافع اقتصادی و اجتماعی نهادها در استفاده از کنترلگرهایی است که مایل به توافق با شرایط قراردادی الزام‌آور برای انطباق با اقدامات امنیتی متناسب‌اند. علاوه بر این، نهادها اگر از خدمات کنترلگرها استفاده نمایند، به احتمال کمتری مسئول اقدامات یا خسارات ناشی از پردازش می‌باشند. اما در هر حال، همان‌طور که در بالا اشاره شد، الزامات امنیتی مندرج در مادۀ ۳۲، صرف‌نظر از اینکه در قرارداد ذکر شوند یا خیر، به طور مستقیم به پردازشگر و کنترلگر هر دو بار می‌شود.

۳.۲.۲. امنیت داده‌ها تحت لایحه

الزامات امنیتی داده در مادۀ ۲۸ لایحه نیز به طور مساوی در مورد کنترلگر و پردازشگر اعمال می‌شود؛ هر دوی آنها ملزم به مطابقت با تمهیدات ایمنی و امنیتی مادۀ مذکورند. هریک از کارکردها و مراحل پردازش، باید از تمهیدات ایمنی و امنیتی ویژه خود برخوردار باشند. این تمهیدات باید هر سه سطح ۱) ایمنی و حفاظت فیزیکی؛ ۲) ایمنی و حفاظت اطلاعات و ۳) ایمنی و حفاظت انسانی را دربرگیرند. مطابق مادۀ ۳۰، اشخاص موضوع داده در صورتی‌که هزینه‌های تمهیدات ایمنی و حفاظتی فراتر را به کنترلگر یا پردازشگر پرداخت کنند و اجرای آن تمهیدات ایفای تعهدات آنها را مختل نکند، می‌توانند تمهیدات ایمنی و حفاظتی فراتر را نیز خواستار شوند. مشابه حکم این ماده به صراحت در GDPR نیامده است.

۱. ماده ۲۸، بند ۳، پاراگراف c .

۴. شک در عنوان قانونی کنترلگر یا پردازشگر

با توجه به اینکه در خلال عملیات پردازش داده‌ها، مخصوصاً در متن لایحه بیشترین مسئولیت بر کنترلگر بار شده است و این رویه هرچند به گونه‌ای تعدیل شده است، در GDPR نیز جاری است. اصل حفاظت حداکثری از داده‌های شخصی و حقوق افراد موضوع داده اقتضا دارد تا در مواقع شک در تشخیص کنترلگری یا پردازشگری، قائل بر کنترلگر بودن نقش مشکوک باشیم، این تفسیر مطابق با نظریهٔ گزیده شده توسط دیوان اتحادیه اروپا[1] و دیوان دادگستری اروپا است.[2]

1. judgment of 13 May 2014, Google Spain, C 131/12, EU:C:2014:317, Available at : http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 (last visited on 05/10/ 2019), paragraph 34.

2.ttp://curia.europa.eu/juris/document/document.jsf;jsessionid=9D9DF361570E7E8B252244680A1AC3F2?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=291951).

نتیجه‌گیری

با مقایسهٔ لایحه با GDPR متن لایحه از نظر ادبیات قانون‌نویسی و مشخص نمودن تفصیلی تکالیف و مسئولیت‌ها، دارای ضعف‌های آشکاری می‌باشد. در GDPR و لایحه استفاده از خدمات یک ارائه‌دهندهٔ پردازشگر یا کنترلگر، هر کدام مزایا و معایب خاص خود را دارد. در هر دو متن نهادی که قصد بهره‌گیری از خدمات پردازش داده را دارد، بدواً تعهدی اولیه و مسئولیت‌زا در راستای دقت در انتخاب ارائه‌دهنده خدمات دارند. بر خلاف لایحه در GDPR در مواردی بر انعقاد قرارداد برای روشن شدن و تصریح بر مسئولیت‌ها تاکید شده است. در هر دو متن، اگر ارائه‌دهنده شخص ثالث یک پردازشگر باشد، نهادها معمولاً کنترل و مسئولیت بیشتری نسبت به نحوهٔ پردازش اطلاعات دارند. واگذاری خدمات به یک کنترلگر حداقل در برخی موارد می‌تواند برای حفظ حریم خصوصی افراد بهتر باشد. اگر ارائه‌دهندهٔ خدمات یک کنترلگر باشد، برخلاف ظاهر لایحه، مطابق GDPR نهاد متقاضی ممکن است از تعهدات مربوطه از قبیل ارائهٔ اطلاعات حریم‌خصوصی به افراد موضوع داده، یا پاسخگویی به افراد موضوع داده که درخواست اعمال حقوق خود را دارند، اطلاعیه‌ها و مسئولیت‌های نظارتی در مورد رویداد نقص و آماده‌سازی ارزیابی تأثیر حفاظت از داده‌ها برای پردازش با ریسک بالا معاف گردد. در این حالت، نهاد متقاضی کمتر احتمال دارد که برای نقض در عملیاتی که از یک کنترلگر مستقل استفاده نموده است، مسئولیتی داشته باشد. این عوامل باید در استفاده از محصولات یا خدماتی که شامل جمع‌آوری داده‌ها توسط یک ارائه‌دهندهٔ ثالث می‌شوند، در نظر گرفته شوند. در کل می‌توان نتیجه گرفت که در تحت هر دو سند مورد مطالعه بهتر است از نظر اطمینان به افراد موضوع داده و رهایی از تعهدات سنگین کنترلگری، نهاد متقاضی از خدمات ارائه‌شده توسط کنترلگر مستقل استفاده کند.

پیشنهاد می‌شود در هر دو متن مورد مطالعه جای خالی تعریف و مسئولیت‌انگاری صریح نهاد متقاضی پردازش احساس می‌شود. لذا ما پیشنهاد می‌کنیم موارد ذیل به لایحه الحاق گردد:

الف) تعریف: نهاد متقاضی پردازش هر نهاد عمومی، دولتی یا غیر دولتی یا شخص حقیقی یا حقوقی است که قصد انجام عملیات پردازش با استفاده از خدمات پردازشگر یا کنترلگر بر روی داده‌های متعلق به مراجعان، مشتریان یا هرگونه داده‌ای را که به هر دلیلی در اختیار وی قرار دارد یا قرار می‌گیرد، دارد.

ب) تعهدات: ۱) اگر شخص طرف قرار داد یک کنترلگر باشد کـه تمـامی تعهـدات کنترلگـری را به‌طور مستقل بپذیرد و نهاد متقاضی هیچ دخالتی در امر کنترلگری نداشته باشـد، مسـئولیت پردازش مطابق این قانون با کنترلگر و دیگر اشخاص درگیر اسـت و نهـاد متقاضـی در ایـن فرض به مثابه یک کارفرما صرفاً در حد اطمینان از تعهدپذیری و اعتبار طرف مستقیم قرارداد تعهد دارد.

۲) چنانچه شخص طرف قرار داد یک کنترلگر باشد که تعهدات کنترلگری را بپـذیرد، ولـی نهـاد متقاضی در امر کنترلگری حضور داشته باشد یا مداخله نماید، نهاد متقاضی و کنترلگر هـر دو کنترلگر مشترک شناخته می‌شوند و مسئولیت پردازش مطابق این قانون برای هر دو، با دیگر اشخاص درگیر در پردازش است، به علاوه نهاد متقاضی در این فـرض مسـئول اطمینـان از تعهدپذیری و اعتبار طرف قرارداد نیز می‌باشد.

۳) چنانچه شخص طرف قرارداد یک پردازشگر باشد، نهاد متقاضی امر، کنترلگر به حساب می‌آید و دارای کلیه تعهدات کنترلگری است؛ در این فرض نیز مسـئول اطمینـان از تعهدپـذیری و اعتبار طرف قرارداد می‌باشد.

فهرست منابع

الف) منابع فارسی

کتاب

۱. اصلانی، حمیدرضا، ***حقوق فناوری اطلاعات***، تهران: میزان. ۱۳۸۹.

۲. جعفری لنگرودی، محمد جعفر، ***مبسوط در ترمینولوژی حقوق***، تهران: گنج دانش، ۱۳۸۷.

۳. قاجار قیونلو، سیامک، ***مقدمه حقوق سایبر***، تهران: میزان، ۱۳۹۱.

مقاله

۴. باقری، احمد و مریم حجتی، **بررسی تعهدات امین در فقه امامیه و حقوق موضوعه**، پژوهش‌های فقهی، زمستان ۱۳۹۳، شماره ۴، صص ۶۵۹ -۶۷۶.

۵. پدرام، سعید و حمیدرضا رحمانی‌زاده دهکردی، **شفاف‌سازی و پاسخگویی در نهادهای رسمی، مجلس و راهبرد**، زمستان ۱۳۸۱، شماره ۳۶، صص ۸۵-۹۵.

۶. جان‌نثاری، اعظم، فاطمه ترابی و فاطمه علی نجیبی‌نیا، **تحول عظیم ابرداده‌ها و بررسی چالش‌های آن، برلین: سومین کنفرانس بین‌المللی پژوهش در علوم و تکنولوژی**، ۱۳۹۵.

۷. فروغی، فضل الله، محمدناصر برجی و جواد مصلحی، **مبانی ممنوعیت نقض حریم خصوصی در حقوق ایران و آمریکا**، مطالعات حقوقی، پاییز ۱۳۹۳، شماره ۳، صص۱۳۷-۱۷۲.

۸. قنواتی، جلیل و حسین جاور، **حریم خصوصی؛ حق یا حکم**، مجله حقوق اسلامی، زمستان ۱۳۹۰، شماره ۳۱ : ۷-۳۲، ص۲۷.

اسناد

۹. قانون تجارت الکترونیک.

۱۰. لایحه صیانت و حفاظت از داده‌های شخصی.

ب) منابع انگلیسی

Articles

i. Esayas, S.” The Role of Anonymisation and Pseudonymisation Under the EU Data Privacy Rules: Beyond the ‘All or Nothing”. European Journal of Law and Technology, Vol 6, No 2, 2015.

11. Hintze M,” In Defense of the Long Privacy Statement”. Maryland Law Review. 76 .1044. 2017.
12. Daecher A, Cotteleer M, Holdowsky. J.”The Internet of Things: A technical primer”. 2018 , available at: https://www2.deloitte.com/insights/us/en/focus/internet-of-things/technical-primer.html?icid=dcom_promo_featured|us;en (last visited on 25/012/ 2018).
13. Layton, R, “How the GDPR Compares to Best Practices for Privacy, Accountability and Trust” (March 31, 2017). Available at SSRN: https://ssrn.com/abstract=2944358 or http://dx.doi.org/10.2139/ssrn.2944358(last visited on 20/12/ 2018) .
14. Stanescu, C. G. and Ievchuk, N, Alexa, Where Is My Private Data? Unanswered Legal and Ethical Questions Regarding Protection and Sharing of Private Data Collected and Stored by Virtual Private Assistants (May 3, 2018). Available at: SSRN: https://ssrn.com/abstract=3250669(last visited on 17/08/ 2019).
15. An official website of the European Union “ Protection of Personal Data - European Commission,” EU, accessed August 25, 2017, http://ec.europa.eu/justice/data-protection/.(last visited on 11/8/ 2019).

Cases

16. judgment of 13 May 2014,” Google Spain”, C 131/12, EU:C:2014:317, Available at : http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065
17. (last visited on 05/10/ 2019).
18. Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of 'controller' and 'processor'" (WP 169), adopted on 16 February 2010, at 9. (last visited on 09/11/ 2019) .

Internet Sites

19. http://curia.europa.eu/juris/document/document.jsf;jsessionid (last visited on 18/05/ 2019) = 9D9DF361570E7E8B252244680A1AC3F2? text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ =first&part=1&cid=291951(last visited on 1/06/ 2019).
20. http://ec.europa.eu/justice/data-protection (last visited on 1/06/ 2019).
21. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679(last visited on 1/06/ 2019).
22. https://GDPR -info.eu/recitals/no-109/(last visited on 3/06/ 2019).
23. https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf . (last visited on 12/06/ 2019).
24. https://www.newyorker.com/tech/elements/the-GDPR -europes-new-privacy- law-and-thefuture- of-the-global-data-economy.
25. https://www.nytimes.com/2018/05/24/technology/europe-GDPR -privacy.html (last visited on 12/06/ 2019).
26. https://www.privacyshield.gov(last visited on 12/06/ 2019).

Documents

27. APEC PRIVACY FRAMEWORK (2015) . Available at: https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015) (last visited on 1/06/ 2019).
28. General Data Protection Regulation . Available at: https://eur-lex.europa.eu/legalcontent/EN/TXT/? uri= CELEX: 32016R0679 (last visited on 1/06/ 2019).
29. Data Protection Act 2018 Available at: https://ico.org.uk/for-organisations/data-protection-act-2018/(last visited on 1/06/ 2019)
30. Data Protection Act 1998 Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents(last visited on 1/06/ 2019).