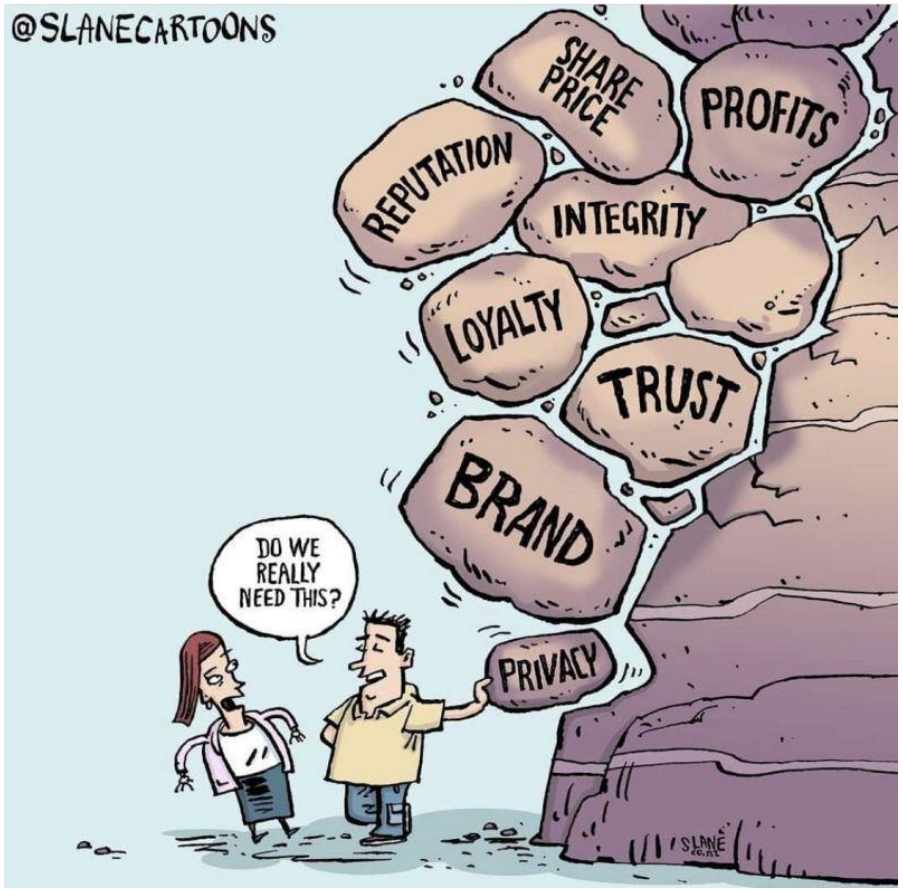
Data Privacy специфика | Алексей Мунтян
при использовании DLP | *Редакция от 13.07.2022*



Алексей Мунтян, *13 лет в Data Privacy*

Основатель и CEO в компании Privacy Advocates

Соучредитель и член Правления в Russian Privacy Professionals Association - RPPA.ru

Внешний Data Protection Officer в двух транснациональных холдингах

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru

Моя визитка

3

Что необходимо учитывать при внедрении и использовании DLP-систем или иного мониторинга

- ст.23(1) - Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
- ст.23(2) - Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

- ст.86(3) - получение персональных данных не от самого работника
- ст.88(1) - сообщение персональных данных работника третьей стороне

- ст.16 - принятие решений на основании исключительно автоматизированной обработки персональных данных

- ст.138(1) - нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан…
- ст.138(2) - то же деяние, совершенное лицом с использованием своего служебного положения…

➢ Разъяснения Роскомнадзора от 14.12.2012 относительно вопросов, касающихся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве

Свод практических правил по защите персональных данных работников, принятый Международной организацией труда в 1997 году

5. Общие принципы

5.4. Персональные данные, собранные в связи с техническими или организационными мерами обеспечения безопасности и надлежащей работы автоматизированных информационных систем, не должны использоваться для контроля за поведением работников.

5.5. Решения, касающиеся работника, не могут основываться исключительно на автоматизированной обработке персональных данных работника.

5.6. Персональные данные, собранные с помощью электронного мониторинга, не должны быть единственными факторами при оценке эффективности работы.

5.7. Работодатели должны регулярно оценивать свои методы обработки данных:

(a) сократить, насколько это возможно, формы и количество собираемых персональных данных;

(b) совершенствовать способы защиты личной жизни работников.

5.8. Работников и их представителей следует информировать о любом процессе сбора данных, о правилах, регулирующих этот процесс, и об их правах...

5.13. Работники не могут отказаться от своих прав на личную жизнь...

6. Сбор персональных данных

6.1. Все персональные данные в принципе должны быть получены от конкретного работника...

6.14. (1) В случае контроля за деятельностью работников они должны быть заранее информированы о его проведении, расписании, используемых методах и технологиях, а также о собираемых данных, и работодатель должен свести к минимуму вторжение в личную жизнь работников.

(2) Тайный контроль может быть разрешен только, если:

(a) он соответствует внутригосударственному законодательству, или

(b) существуют разумные основания подозревать наличие преступной деятельности либо других серьезных правонарушений.

(3) Непрерывный контроль может быть разрешен только по соображениям охраны здоровья и обеспечения безопасности или для защиты имущества...

Рекомендация Комитета министров Совета Европы государствам-участникам об обработке персональных данных в контексте занятости CM/Rec(2015)5 от 01.04.2015

10.3. Следует дать особо четкое и полное описание категорий персональных данных, которые могут быть собраны посредством информационно-коммуникационных технологий, включая видеонаблюдение, а также их возможного использования. Этот принцип также применим к некоторым формам обработки данных, предусмотренным в части II Приложения к настоящей рекомендации.

10.4. Информация должна предоставляться в доступной форме. В любом случае данная информация должна предоставляться до того, как работник осуществит деятельность или предпримет соответствующие действия, а также она должна быть легко доступна через информационные системы, обычно используемые работником...

14. Использование Интернета и электронных коммуникаций на рабочем месте

14.1. Работодатели должны избегать незаконных и необоснованных вмешательств в право работников на личную жизнь. Данный принцип распространяется на все технологические устройства и информационно-коммуникационные технологии, используемые работодателем. В порядке осуществления четкой политики конфиденциальности следует периодически информировать соответствующие лица о ясной политике сохранения приватности, в соответствии с принципом 10 настоящей рекомендации. Предоставленная информация должна постоянно обновляться и должна преследовать цель обработки данных, их хранения или периодического резервного копирования данных трафика и архивирования профессиональных электронных сообщений.

14.2. В частности, в случае обработки персональных данных, касающихся Интернета или интернет-страниц, доступных для работника, предпочтение следует отдавать принятию превентивных мер, таких как использование фильтров, которые препятствуют выполнению конкретных операций, а также классификации возможных механизмов контроля персональных данных, отдавая предпочтение неиндивидуальным выборочным проверкам данных, которые являются анонимными или в каком-то смысле имеют обобщенный характер.

14.3. Доступ работодателей к служебным электронным сообщениям своих работников, которых заранее уведомили о такой возможности, может иметь место, только когда это необходимо по соображениям безопасности или другим законным основаниям. В случае отсутствия работников на рабочем месте работодатели должны принять все необходимые меры и предусмотреть соответствующие процедуры, имеющие целью получение доступа к профессиональным электронным сообщениям, только когда такой доступ является профессиональной необходимостью. Доступ должен осуществляться с минимальным вмешательством и только после информирования соответствующих работников.

14.4. Содержание, отправка и получение личных электронных сообщений на работе не должны контролироваться ни при каких обстоятельствах.

14.5. При увольнении работника из организации работодатель должен принять все необходимые организационные и технические меры для автоматической деактивации учетной записи электронных сообщений работника. Если работодателям необходимо восстановить содержание учетной записи работника для эффективного функционирования организации, они должны сделать это до его или ее ухода и, если это возможно, в его или ее присутствии...

Решения ЕСПЧ по делам Bărbulescu v. Romania и Ribalda v. Spain

- Любая переписка работника, в том числе с использованием сервиса корпоративной электронной почты, считается конфиденциальной (нет разницы между приватностью электронных сообщений, сделанных на корпоративных или личных устройствах).
- Требуется определить необходимость (обоснованность) в достижении заявленной цели путем мониторинга поведения работника, а также имелись ли законные основания, оправдывающие наблюдение за сообщениями работника.
- Необходимо обеспечивать надлежащую защиту права работника на уважение его личной жизни и корреспонденции и, следовательно, устанавливать справедливый баланс между интересами работника и работодателя.
- Следует оценивать, могла ли поставленная работодателем цель быть достигнута менее агрессивными методами, чем оценка фактического содержания писем работника.
- Должна быть возможность обжаловать подлинность доказательств, полученных путем мониторинга, и возражать против их применения. Кроме того, должны учитываться качество доказательств, а также обстоятельства их получения, и не бросают ли эти обстоятельства тень на надежность или точность доказательств.

Глава организации в Тынде предстанет перед судом за незаконный сбор персональных данных сотрудника

🔦 По версии следствия, в декабре 2019 года руководитель одной из Тындинских организаций, подозревая своего подчиненного в должностных нарушениях, скрытно установил в его кабинете диктофон, после чего прослушивал незаконно собранную информацию, сохраняя на своем компьютере.

🎤 Таким способом информация незаконно собиралась более двух лет. Каких-либо нарушений в действиях своего подчиненного руководитель не выявил, однако незаконно получил сведения о его частной жизни, в том числе о здоровье сотрудника и здоровье членов его семьи, о конфликтах и проблемах в семье.

☠️ Теперь руководитель обвиняется в совершении преступления, предусмотренного ч. 2 ст. 137 УК РФ (незаконное собирание сведений о частной жизни лица, составляющих его личную и семейную тайну, без его согласия, совершенные лицом с использованием своего служебного положения).

🥷 Преступление выявили сотрудники УФСБ России по Амурской области.

https://epp.genproc.gov.ru/web/proc_28/mass-media/news?item=73784816

Российская судебная практика

- Допустимость доказательств, полученных путем мониторинга поведения работников (см. судебные споры об увольнениях за разглашение коммерческой тайны и персональных данных или, например, решение Преображенского районного суда г. Москвы от 27.09.2011 № 2-2958/2011 о признании незаконным увольнение работника за нецелевое использование ресурсов сети Интернет)
- Аргументы касающиеся неприкосновенности частной жизни не работают (см. определение Верховного Суда Республики Хакасия от 29.01.2018 г. по делу №33-33/2018), но важно понимать, что мониторинг – это не перлюстрация (от лат. perlustro – «обозреваю»), т.е. просмотр личной пересылаемой корреспонденции, совершаемый в тайне от отправителя и получателя.

9 Что необходимо сделать перед внедрением DLP

- ✓ всегда учитывать принципы приватности независимо от используемых технологий мониторинга
- ✓ четко обозначить цель мониторинга, обосновать его необходимость и область применения
- ✓ произвести оценку баланса интересов (работник и работодатель) при осуществлении мониторинга
- ✓ оценить пропорциональность (соразмерность) интенсивности («агрессивности») мониторинга, его целей и прав работника
- ✓ определить сценарии и порядок использования сведений, полученных в результате мониторинга, а также возможные юридические последствия для работника (см. допустимость доказательств) в связи с применением мониторинга
- ✓ предоставить работнику (организации по представительству работников) полную информацию о мониторинге до его начала путем ознакомления с соответствующим(и) ЛНА работодателя
- ✓ определить правовое основание для мониторинга (согласие работника, трудовой договор, законный интерес работодателя) и обеспечить его наличие

10 Гарантии и компенсирующие меры при использовании DLP

- ✓ соблюдение принципа минимизации обработки данных (категории, доступ, срок хранения), получаемых посредством мониторинга
- ✓ детальное и понятное для работника описание принципов и правил работы мониторинга
- ✓ мониторинг может иметь скрытый для работника характер только в исключительных случаях
- ✓ некоторые меры мониторинга не должны происходить в отсутствие работника
- ✓ запрет на использование результатов мониторинга любым способом, отличным от указанного в ЛНА
- ✓ приоритетность средств фильтров, ограничений и блокировки (например, публичных почтовых сервисов, интернет-месседжеров, социальных сетей и других ресурсов) над средствами постоянного мониторинга (включая автоматическое копирование, перехват и чтение сообщений, направляемых работнику)
- ✓ предоставление возможности работнику отказаться от действия (например, отправления письма), которое по своим признакам может быть отнесено к нарушению безопасности информации (data breach)
- ✓ соблюдение принципа «четырех глаз» (four eyes principle) в процессе принятия решений на основании результатов мониторинга
- ✓ ПО для записи и снимков экранов, записи движения мыши, записи нажатия клавиш клавиатуры, записи с веб-камер, журналирования использования приложений должно использоваться в исключительных случаях
- ✓ регулярное уведомление работника об осуществлении мониторинга (например, автоматическое предупреждение работника о записи телефонного разговора)

11 Рекомендации по содержанию ЛНА о применении DLP

- цель мониторинга, область его применения (например, электронная почта, интернет-мессенджеры, файлы на файл-серверах и в системах хранения данных, приложениях коллективного пользования, записи в базах данных, телефонные переговоры и т.п.) и методы осуществления
- описание обработки данных, осуществляемой в ходе контроля (состав данных, действия с ними, источники их получения, длительность их хранения, вовлечение третьих лиц в обработку)
- описание прав и обязанностей работника при осуществлении мониторинга
- описание возможных юридических последствий для работника в связи с применением мониторинга
- особенности и ограничения в использовании работником предоставленных работодателем и собственных устройств и ресурсов для обработки данных в рабочих и личных целях, например:
  - указание на то, что служебные средства обработки информации принадлежат работодателю, а работник не может рассчитывать на конфиденциальность своих сообщений и отправлений;
  - регламентация допустимого объема передаваемых сообщений, видов файлов, разрешенных (запрещенных) к передаче, порядка рассылки многоадресных, рекламных и материалов и т.п.;
  - запрет на отправление по незащищенным каналам связи информации ограниченного доступа, а также использование СЗИ, не принятых в эксплуатацию установленным порядком.
- установление запрета на противодействие (воспрепятствование) мониторингу со стороны работника

Есть ли альтернатива согласию как базовому способу легитимизации обработки данных работника?

Согласие на обработку персональных данных - Pros v Cons

- ✓ Простой для понимания концепт
- ✓ Нравится надзорным органам

- ➢ Не все готовы предоставить
- ➢ Может быть отозвано в любой момент
- ➢ Ресурсы и время для получения
- ➢ Бремя администрирования и хранения
- ➢ Иллюзии работника о контроле

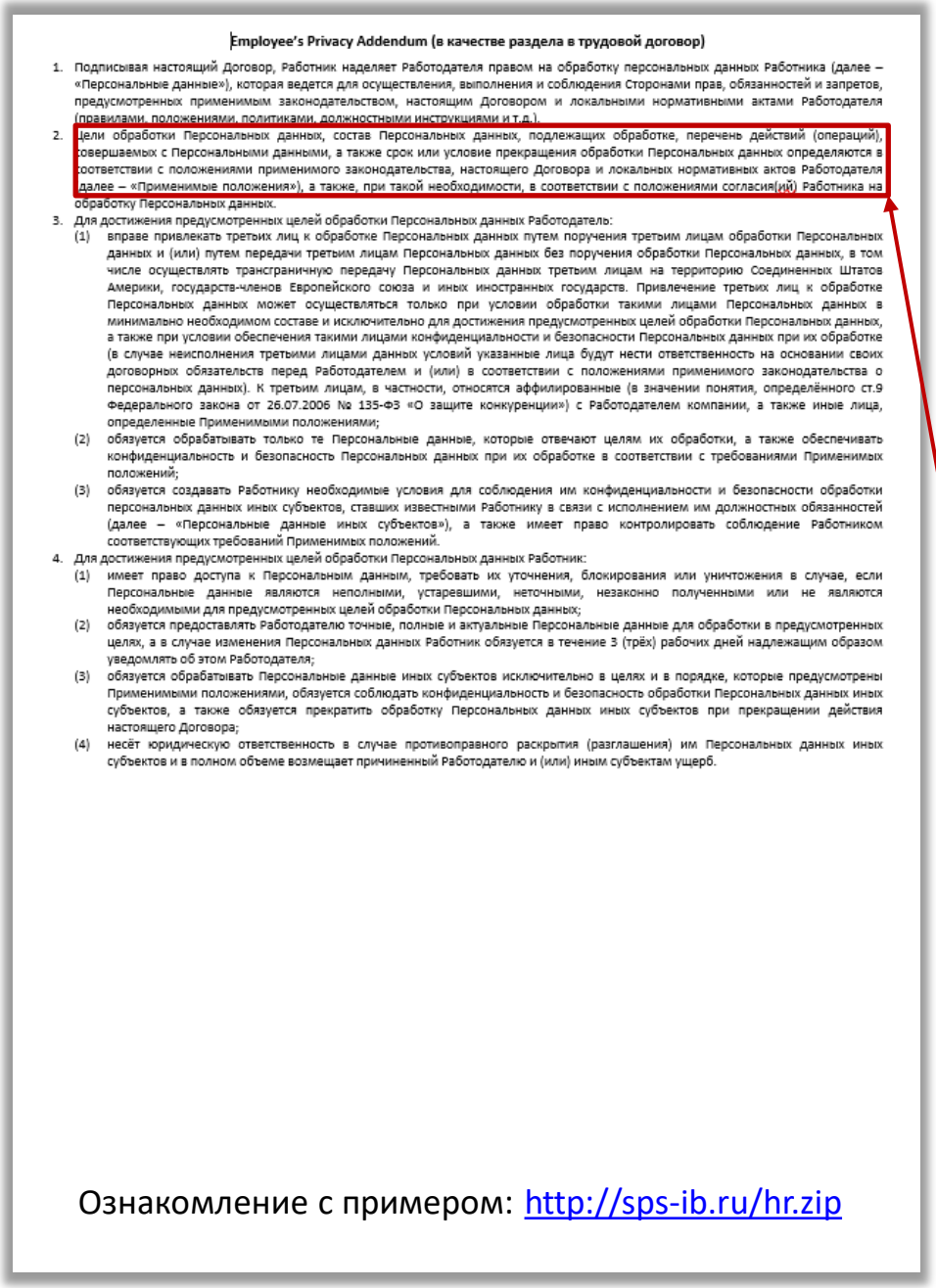
*Связка **ТД+ЛНА** как более рискованная, но удобная альтернатива получению согласий*

Согласно ст.6(1)(5) и ст.6(1)(7) 152-ФЗ допускается обработка персональных данных без письменного согласия работника, если она **необходима для исполнения договора**, стороной которого является работник, для осуществления **прав и законных интересов работодателя** или третьих лиц при условии, что при этом не нарушаются права и свободы работника. Вышеизложенные нормы права содержат основания для обработки персональных данных без применения общих норм о получении согласия субъекта персональных данных.

Также важные следующие положения Трудового кодекса РФ:

- ст.15 - трудовые отношения основаны на **соглашении между работником и работодателем** о личном выполнении работником за плату трудовой функции в интересах, под управлением и контролем работодателя, подчинении работника правилам внутреннего трудового распорядка;
- ст.21 - работник обязан добросовестно исполнять свои трудовые обязанности, возложенные на него трудовым договором, и соблюдать правила внутреннего трудового распорядка;
- ст.22 - работодатель вправе принимать **локальные нормативные акты, содержащие нормы трудового права**, а также требовать от работников исполнения ими трудовых обязанностей и соблюдения правил внутреннего трудового распорядка.

13 Пример privacy-раздела в трудовом договоре



Employee's Privacy Addendum (в качестве раздела в трудовой договор)

1. Подписывая настоящий Договор, Работник наделяет Работодателя правом на обработку персональных данных Работника (далее – «Персональные данные»), которая ведется для осуществления, выполнения и соблюдения Сторонами прав, обязанностей и запретов, предусмотренных применимым законодательством, настоящим Договором и локальными нормативными актами Работодателя (правилами, положениями, политиками, должностными инструкциями и т.д.).
2. Цели обработки Персональных данных, состав Персональных данных, подлежащих обработке, перечень действий (операций), совершаемых с Персональными данными, а также срок или условие прекращения обработки Персональных данных определяются в соответствии с положениями применимого законодательства, настоящего Договора и локальных нормативных актов Работодателя (далее – «Применимые положения»), а также, при такой необходимости, в соответствии с положениями согласия(ий) Работника на обработку Персональных данных.
3. Для достижения предусмотренных целей обработки Персональных данных Работодатель:
   (1) вправе привлекать третьих лиц к обработке Персональных данных путем поручения третьим лицам обработки Персональных данных и (или) путем передачи третьим лицам Персональных данных без поручения обработки Персональных данных, в том числе осуществлять трансграничную передачу Персональных данных третьим лицам на территорию Соединенных Штатов Америки, государств-членов Европейского союза и иных иностранных государств. Привлечение третьих лиц к обработке Персональных данных может осуществляться только при условии обработки такими лицами Персональных данных в минимально необходимом составе и исключительно для достижения предусмотренных целей обработки Персональных данных, а также при условии обеспечения такими лицами конфиденциальности и безопасности Персональных данных при их обработке (в случае неисполнения третьими лицами данных условий указанные лица будут нести ответственность на основании своих договорных обязательств перед Работодателем и (или) в соответствии с положениями применимого законодательства о персональных данных). К третьим лицам, в частности, относятся аффилированные (в значении понятия, определённого ст.9 Федерального закона от 26.07.2006 № 135-ФЗ «О защите конкуренции») с Работодателем компании, а также иные лица, определенные Применимыми положениями;
   (2) обязуется обрабатывать только те Персональные данные, которые отвечают целям их обработки, а также обеспечивать конфиденциальность и безопасность Персональных данных при их обработке в соответствии с требованиями Применимых положений;
   (3) обязуется создавать Работнику необходимые условия для соблюдения им конфиденциальности и безопасности обработки персональных данных иных субъектов, ставших известными Работнику в связи с исполнением им должностных обязанностей (далее – «Персональные данные иных субъектов»), а также имеет право контролировать соблюдение Работником соответствующих требований Применимых положений.
4. Для достижения предусмотренных целей обработки Персональных данных Работник:
   (1) имеет право доступа к Персональным данным, требовать их уточнения, блокирования или уничтожения в случае, если Персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для предусмотренных целей обработки Персональных данных;
   (2) обязуется предоставлять Работодателю точные, полные и актуальные Персональные данные для обработки в предусмотренных целях, а в случае изменения Персональных данных Работник обязуется в течение 3 (трёх) рабочих дней надлежащим образом уведомлять об этом Работодателя;
   (3) обязуется обрабатывать Персональные данные иных субъектов исключительно в целях и в порядке, которые предусмотрены Применимыми положениями, обязуется соблюдать конфиденциальность и безопасность обработки Персональных данных иных субъектов, а также обязуется прекратить обработку Персональных данных иных субъектов при прекращении действия настоящего Договора;
   (4) несёт юридическую ответственность в случае противоправного раскрытия (разглашения) им Персональных данных иных субъектов и в полном объеме возмещает причиненный Работодателю и (или) иным субъектам ущерб.

Цели обработки Персональных данных, состав Персональных данных, подлежащих обработке, перечень действий (операций), совершаемых с Персональными данными, а также срок или условие прекращения обработки Персональных данных определяются в соответствии с положениями применимого законодательства, настоящего Договора и локальных нормативных актов Работодателя, а также, при такой необходимости, в соответствии с положениями согласия(ий) Работника на обработку Персональных данных.

Ознакомление с примером: http://sps-ib.ru/hr.zip

Пример privacy-раздела в ЛНА об использовании служебных автомобилей

Privacy-раздел в локальный нормативный акт (на примере «Политики по использованию корпоративных автомобилей»)

1. Путем ознакомления под роспись с Политикой Пользователь соглашается с необходимостью обработки Компанией его персональных данных и наделяет Компанию правом на их обработку с целью предоставления Пользователю Автомобиля (служебного транспортного средства), учета и возмещения расходов на эксплуатацию автомобиля, контроля надлежащего использования и сохранности Автомобиля.
2. Компания вправе осуществлять с использованием средств автоматизации и без использования средств автоматизации такие действия как сбор, получение от третьих лиц (органов государственной власти, поставщиков информационно-справочных услуг в сфере привлечения к административной ответственности за нарушение правил дорожного движения, поставщиков услуг по аренде (лизингу) транспортных средств, поставщиков услуг по отслеживанию режима использования и эксплуатации транспортных средств, иных заинтересованных лиц), анализ, поиск, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (доступ), блокирование, удаление, уничтожение нижеуказанных персональных данных Пользователя (далее – «Персональные данные») в рамках достижения зафиксированной в Политике цели обработки Персональных данных:
   - 2.1. фамилия, имя, отчество
   - 2.2. дата рождения
   - 2.3. номер контактного телефона
   - 2.4. адрес электронной почты
   - 2.5. наименование должности
   - 2.6. наименование структурного подразделения
   - 2.7. наименование и адрес текущего места трудоустройства
   - 2.8. зарегистрированный адрес действительного места жительства
   - 2.9. дата регистрации по месту жительства
   - 2.10. фактический адрес действительного места жительства
   - 2.11. наименование и реквизиты (серия и номер, дата выдачи, наименование и код выдавшего органа) документа, удостоверяющего личность лица на территории Российской Федерации
   - 2.12. сведения о факте предоставления Автомобиля, о допуске к управлению Автомобилем и о периоде использования (эксплуатации) Автомобиля
   - 2.13. сведения о факте, об обстоятельствах и о размере причиненных Автомобилю повреждений или иного ущерба
   - 2.14. сведения (дата, основание) о продаже (передаче) Автомобиля Пользователю
   - 2.15. сведения о наличии права управления транспортными средствами
   - 2.16. сведения о наличии (об отсутствии) медицинских противопоказаний, медицинских показаний или медицинских ограничений к управлению транспортными средствами
   - 2.17. реквизиты (страна выдачи, серия и номер, дата выдачи, дата окончания срока действия, наименование и код выдавшего органа) удостоверения на право управления транспортными средствами
   - 2.18. сведения о категориях, подкатегориях транспортных средств, на право управления которыми выдано удостоверение, а также дата получения такого права
   - 2.19. сведения о стаже управления транспортными средствами
   - 2.20. сведения о навыках управления транспортными средствами, а также о знаниях и степени соблюдения правил дорожного движения
   - 2.21. сведения о расходах на эксплуатацию Автомобиля
   - 2.22. сведения о скорости, ускорении, расходе топлива, пробеге Автомобиля, а также об использовании средств пассивной безопасности и светотехники Автомобиля
   - 2.23. сведения о манере управления Автомобилем и о соблюдении корпоративных правил безопасного управления Автомобилем
   - 2.24. сведения об использовании услуг платной парковки Автомобиля
   - 2.25. сведения о факте и об обстоятельствах правонарушения, совершенного с использованием Автомобиля
   - 2.26. изображения[1] Автомобиля и (или) находящихся в нем лиц[2], подтверждающее наличие (отсутствие) события правонарушения, совершенного с использованием Автомобиля
   - 2.27. сведения о привлечении к юридической ответственности за правонарушения, совершенные с использованием Автомобиля
   - 2.28. государственный регистрационный номер Автомобиля
   - 2.29. марка и модель Автомобиля
   - 2.30. идентификационный номер Автомобиля (VIN)
   - 2.31. номера основного компонента Автомобиля (кузова, рамы, кабины, шасси)
   - 2.32. сведения (модель, номер, мощность, рабочий объем, тип) о двигателе Автомобиля
   - 2.33. сведения о типе, категории, годе изготовления, организации-изготовителе, цвете, массе, экологическом классе и стране вывоза Автомобиля
   - 2.34. сведения о комплектации, стоимости, технических характеристиках и техническом состоянии Автомобиля
   - 2.35. сведения о факте и дате снятия с регистрационного учета Автомобиля
   - 2.36. реквизиты (серия и номер, дата выдачи, наименование выдавшего органа) паспорта Автомобиля
   - 2.37. реквизиты (серия и номер, дата выдачи, наименование выдавшего органа) свидетельства о государственной регистрации Автомобиля
   - 2.38. сведения о топливной карте (серия и номер, дата выдачи, размер лимитов) и об ее использовании
3. Компания вправе привлекать третьих лиц к обработке Персональных данных путем поручения третьим лицам обработки Персональных данных и (или) путем передачи третьим лицам Персональных данных без поручения обработки Персональных данных, в том числе осуществлять трансграничную передачу Персональных данных третьим лицам на территорию Соединенных Штатов Америки, государств-членов Европейского союза и иных иностранных государств. Привлечение третьих лиц к обработке Персональных данных может осуществляться только при условии обработки такими лицами Персональных данных в минимально необходимом составе и исключительно для достижения предусмотренных целей обработки Персональных данных, а также при условии обеспечения такими лицами конфиденциальности и безопасности Персональных данных при их обработке (в случае неисполнения третьими лицами данных условий указанные лица будут нести ответственность на основании своих договорных обязательств перед Компанией и (или) в соответствии с положениями применимого законодательства о персональных данных). К третьим лицам, в частности, относятся:
   - (1) Общество с ограниченной ответственностью «_____» (адрес:_____), которое является оператором системы управления автопарком «_____»;
   - (2) организации, оказывающие услуги по обязательному страхованию гражданской ответственности владельцев транспортных средств (ОСАГО) и (или) по страхованию транспортных средств от ущерба, хищения или угона (КАСКО);
   - (3) поставщики работ по техническому обслуживанию и ремонту транспортных средств;
   - (4) поставщики услуг по шиномонтажу, ремонту и хранению шин/колес;
   - (5) поставщики услуг выездной технической помощи и эвакуации транспортных средств;
   - (6) поставщики услуг по аренде (лизингу) транспортных средств;
   - (7) автомобильные дилеры;
   - (8) процессинговые центры, эмитирующие топливные карты;
   - (9) поставщики услуг (владельцы) платной парковки транспортных средств.
4. Компания вправе распространять персональные данные Пользователя в объеме, указанном в предоставленной Компанией Пользователю доверенности на управление Автомобилем, путем сообщения любым лицам, заинтересованным в проверке подлинности и действительности такой доверенности.
5. Обработка персональных данных будет осуществляться со дня ознакомления Пользователя под роспись с положениями Политики и до дня прекращения трудовых отношений Пользователя с Компанией, а также после их прекращения в течение 5 (пяти) лет для соблюдения сроков исковой давности и выполнения требований законодательства о налогах и о бухгалтерском учете, в том числе в отношении обработки Персональных данных в информационных системах Компании и системы управления автопарком «_____», при условии, что иное не предусмотрено применимым законодательством или соглашением между Пользователем и Компанией.
6. Пользователю было разъяснено, что в случае его отказа ознакомиться под роспись с Политикой и тем самым наделить Компанию правом на обработку Персональных данных, Компания будет лишена возможности предоставить Пользователю Автомобиль.
7. Пользователь был проинформирован о своем праве получать доступ к Персональным данным, требовать их уточнения, блокирования или уничтожения в случае, если такие персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для достижения зафиксированной в Политике цели обработки Персональных данных. Указанные в настоящем пункте права могут быть реализованы Пользователем либо путем личного предоставления письменного обращения уполномоченному представителю Компании (Менеджеру по транспорту или Руководителю по работе с корпоративным транспортом), либо путем почтового направления письменного обращения по адресу Компании. Обращение, направляемое Компании, должно содержать следующую информацию:
   - (1) сведения об обратившемся лице (фамилия, имя, отчество, адрес места жительства, наименование и номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе);
   - (2) указание на связь обращения с обработкой Персональных данных в рамках Политики;
   - (3) описание предмета обращения (запрос о доступе к Персональным данным; требование уточнения, блокирования или уничтожения Персональных данных);
   - (4) дата составления обращения и подпись обратившегося лица.
8. Фактом своего ознакомления под роспись с Политикой Пользователь подтверждает:
   - (1) что предоставляемые им Компании и (или) уполномоченным ей лицам Персональные данные являются точными, полными и актуальными на момент их предоставления;
   - (2) факт своего ознакомления с условиями обработки Персональных данных и со своими правами как субъекта Персональных данных, а также с возможными последствиями отказа Пользователя ознакомиться под роспись с Политикой и тем самым наделить Компанию правом на обработку Персональных данных.

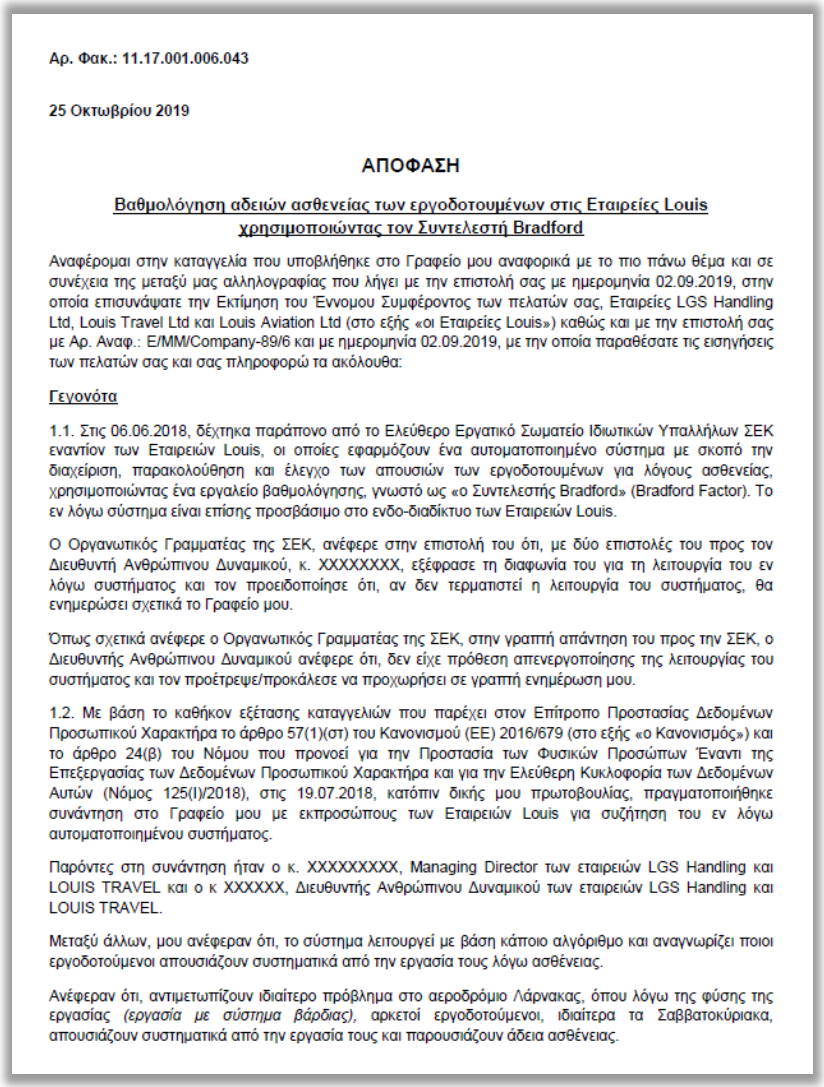
Путем ознакомления под роспись с Политикой Пользователь соглашается с необходимостью обработки Компанией его персональных данных и наделяет Компанию правом на их обработку…

[1] Указанные изображения, созданные работающими в автоматическом режиме специальными техническими средствами, имеющими функции фото- и киносъемки, видеозаписи, или средствами фото- и киносъемки, видеозаписи, могут быть предоставлены Компании самим Пользователем, иными заинтересованными лицами, а также органами государственной власти и поставщиками информационно-справочных услуг в сфере привлечения к административной ответственности за нарушение правил дорожного движения.

[2] Компания не осуществляет действия по обработке изображений находящихся в Автомобиле лиц в качестве биометрических персональных данных и не использует такие изображения для установления личности указанных лиц.

Ознакомление с примером: http://sps-ib.ru/hr.zip

15 Штраф за некорректный LIA



Αρ. Φακ.: 11.17.001.006.043

25 Οκτωβρίου 2019

ΑΠΟΦΑΣΗ

Βαθμολόγηση αδειών ασθενείας των εργοδοτουμένων στις Εταιρείες Louis χρησιμοποιώντας τον Συντελεστή Bradford

Αναφέρομαι στην καταγγελία που υποβλήθηκε στο Γραφείο μου αναφορικά με το πιο πάνω θέμα και σε συνέχεια της μεταξύ μας αλληλογραφίας που λήγει με την επιστολή σας με ημερομηνία 02.09.2019, στην οποία επισυνάψατε την Εκτίμηση του Έννομου Συμφέροντος των πελατών σας, Εταιρείες LGS Handling Ltd, Louis Travel Ltd και Louis Aviation Ltd (στο εξής «οι Εταιρείες Louis») καθώς και με την επιστολή σας με Αρ. Αναφ.: E/MM/Company-89/6 και με ημερομηνία 02.09.2019, με την οποία παραθέσατε τις εισηγήσεις των πελατών σας και σας πληροφορώ τα ακόλουθα:

Γεγονότα

1.1. Στις 06.06.2018, δέχτηκα παράπονο από το Ελεύθερο Εργατικό Σωματείο Ιδιωτικών Υπαλλήλων ΣΕΚ εναντίον των Εταιρειών Louis, οι οποίες εφαρμόζουν ένα αυτοματοποιημένο σύστημα με σκοπό την διαχείριση, παρακολούθηση και έλεγχο των απουσιών των εργοδοτουμένων για λόγους ασθενείας, χρησιμοποιώντας ένα εργαλείο βαθμολόγησης, γνωστό ως «ο Συντελεστής Bradford» (Bradford Factor). Το εν λόγω σύστημα είναι επίσης προσβάσιμο στο ενδο-διαδίκτυο των Εταιρειών Louis.

Ο Οργανωτικός Γραμματέας της ΣΕΚ, ανέφερε στην επιστολή του ότι, με δύο επιστολές του προς τον Διευθυντή Ανθρώπινου Δυναμικού, κ. XXXXXXXX, εξέφρασε τη διαφωνία του για τη λειτουργία του εν λόγω συστήματος και τον προειδοποίησε ότι, αν δεν τερματιστεί η λειτουργία του συστήματος, θα ενημερώσει σχετικά το Γραφείο μου.

Όπως σχετικά ανέφερε ο Οργανωτικός Γραμματέας της ΣΕΚ, στην γραπτή απάντηση του προς την ΣΕΚ, ο Διευθυντής Ανθρώπινου Δυναμικού ανέφερε ότι, δεν είχε πρόθεση απενεργοποίησης της λειτουργίας του συστήματος και τον προέτρεψε/προκάλεσε να προχωρήσει σε γραπτή ενημέρωση μου.

1.2. Με βάση το καθήκον εξέτασης καταγγελιών που παρέχει στον Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα το άρθρο 57(1)(στ) του Κανονισμού (ΕΕ) 2016/679 (στο εξής «ο Κανονισμός») και το άρθρο 24(β) του Νόμου που προνοεί για την Προστασία των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και για την Ελεύθερη Κυκλοφορία των Δεδομένων Αυτών (Νόμος 125(I)/2018), στις 19.07.2018, κατόπιν δικής μου πρωτοβουλίας, πραγματοποιήθηκε συνάντηση στο Γραφείο μου με εκπροσώπους των Εταιρειών Louis για συζήτηση του εν λόγω αυτοματοποιημένου συστήματος.

Παρόντες στη συνάντηση ήταν ο κ. XXXXXXXXX, Managing Director των εταιρειών LGS Handling και LOUIS TRAVEL και ο κ XXXXXX, Διευθυντής Ανθρώπινου Δυναμικού των εταιρειών LGS Handling και LOUIS TRAVEL.

Μεταξύ άλλων, μου ανέφεραν ότι, το σύστημα λειτουργεί με βάση κάποιο αλγόριθμο και αναγνωρίζει ποιοι εργοδοτούμενοι απουσιάζουν συστηματικά από την εργασία τους λόγω ασθένειας.

Ανέφεραν ότι, αντιμετωπίζουν ιδιαίτερο πρόβλημα στο αεροδρόμιο Λάρνακας, όπου λόγω της φύσης της εργασίας *(εργασία με σύστημα βάρδιας)*, αρκετοί εργοδοτούμενοι, ιδιαίτερα τα Σαββατοκύριακα, απουσιάζουν συστηματικά από την εργασία τους και παρουσιάζουν άδεια ασθένειας.

Кто: Γραφείο Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα (Республика Кипр)

Кого: LGS Handling Ltd, Louis Travel Ltd and Louis Aviation Ltd (Louis Group of Companies)

Когда: 2019.10

За что: нарушение ст. 6(1), 9 GDPR

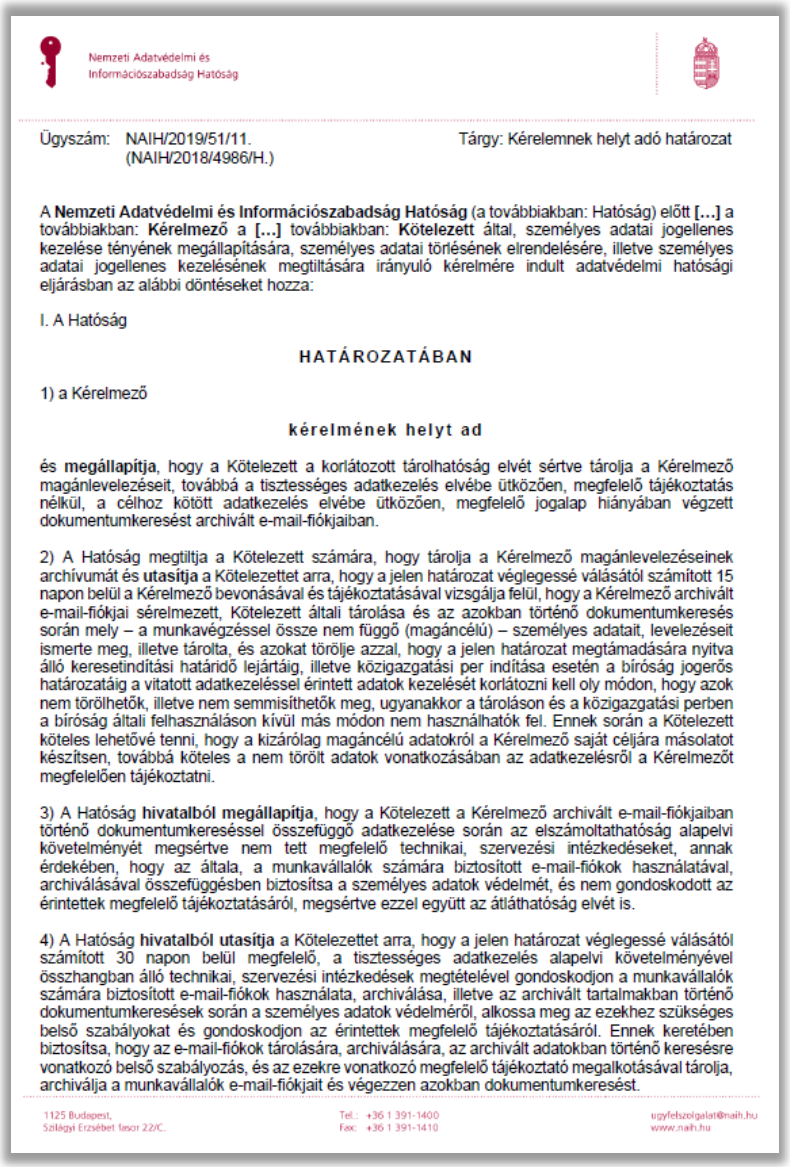
Как: штраф €82,000

Причина: отсутствие правового основания для обработки персональных данных с использованием ПО «Bradford Factor» в целях оценки больничных работников: так, короткие, частые и незапланированные отлучки приводят к большей дезорганизации в компании, чем более длительные.

По мнению надзорного органа, дата и длительность больничного конкретного работника относятся к специальным категориям данных по ст.9(1) GDPR. Хотя контролер провёл DPIA этого процесса и предоставил результаты регулятору для предварительной консультации, но регулятор посчитал, что контролер не смог продемонстрировать баланс своих законных интересов с интересами субъектов (LIA). И как следствие, меры снижения рисков были выбраны некорректно.

https://edpb.europa.eu/news/national-news/2020/cypriot-supervisory-authority-banned-processing-automated-tool-used-scoring_en

Штраф за использование архива корпоративной электронной почты



Nemzeti Adatvédelmi és Információszabadság Hatóság

Ügyszám: NAIH/2019/51/11. (NAIH/2018/4986/H.)

Tárgy: Kérelemnek helyt adó határozat

A **Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: Hatóság) előtt **[...]** a továbbiakban: **Kérelmező** a **[...]** továbbiakban: **Kötelezett** által, személyes adatai jogellenes kezelése tényének megállapítására, személyes adatai törlésének elrendelésére, illetve személyes adatai jogellenes kezelésének megtiltására irányuló kérelmére indult adatvédelmi hatósági eljárásban az alábbi döntéseket hozza:

I. A Hatóság

HATÁROZATÁBAN

1) a Kérelmező

kérelmének helyt ad

és **megállapítja**, hogy a Kötelezett a korlátozott tárolhatóság elvét sértve tárolja a Kérelmező magánlevelezéseit, továbbá a tisztességes adatkezelés elvébe ütközően, megfelelő tájékoztatás nélkül, a célhoz kötött adatkezelés elvébe ütközően, megfelelő jogalap hiányában végzett dokumentumkeresést archivált e-mail-fiókjaiban.

2) A Hatóság megtiltja a Kötelezett számára, hogy tárolja a Kérelmező magánlevelezéseinek archívumát és **utasítja** a Kötelezettet arra, hogy a jelen határozat véglegessé válásától számított 15 napon belül a Kérelmező bevonásával és tájékoztatásával vizsgálja felül, hogy a Kérelmező archivált e-mail-fiókjai sérelmezett, Kötelezett általi tárolása és az azokban történő dokumentumkeresés során mely – a munkavégzéssel össze nem függő (magáncélú) – személyes adatait, levelezéseit ismerte meg, illetve tárolta, és azokat törölje azzal, hogy a jelen határozat megtámadására nyitva álló keresetindítási határidő lejártáig, illetve közigazgatási per indítása esetén a bíróság jogerős határozatáig a vitatott adatkezeléssel érintett adatok kezelését korlátozni kell oly módon, hogy azok nem törölhetők, illetve nem semmisíthetők meg, ugyanakkor a tároláson és a közigazgatási perben a bíróság általi felhasználáson kívül más módon nem használhatók fel. Ennek során a Kötelezett köteles lehetővé tenni, hogy a kizárólag magáncélú adatokról a Kérelmező saját céljára másolatot készítsen, továbbá köteles a nem törölt adatok vonatkozásában az adatkezelésről a Kérelmezőt megfelelően tájékoztatni.

3) A Hatóság **hivatalból megállapítja**, hogy a Kötelezett a Kérelmező archivált e-mail-fiókjaiban történő dokumentumkereséssel összefüggő adatkezelése során az elszámoltathatóság alapelvi követelményét megsértve nem tett megfelelő technikai, szervezési intézkedéseket, annak érdekében, hogy az általa, a munkavállalók számára biztosított e-mail-fiókok használatával, archiválásával összefüggésben biztosítsa a személyes adatok védelmét, és nem gondoskodott az érintettek megfelelő tájékoztatásáról, megsértve ezzel együtt az átláthatóság elvét is.

4) A Hatóság **hivatalból utasítja** a Kötelezettet arra, hogy a jelen határozat véglegessé válásától számított 30 napon belül megfelelő, a tisztességes adatkezelés alapelvi követelményével összhangban álló technikai, szervezési intézkedések megtételével gondoskodjon a munkavállalók számára biztosított e-mail-fiókok használata, archiválása, illetve az archivált tartalmakban történő dokumentumkeresések során a személyes adatok védelméről, alkossa meg az ezekhez szükséges belső szabályokat és gondoskodjon az érintettek megfelelő tájékoztatásáról. Ennek keretében biztosítsa, hogy az e-mail-fiókok tárolására, archiválására, az archivált adatokban történő keresésre vonatkozó belső szabályozás, és az ezekre vonatkozó megfelelő tájékoztató megalkotásával tárolja, archiválja a munkavállalók e-mail-fiókjait és végezzen azokban dokumentumkeresést.

1125 Budapest, Szilágyi Erzsébet fasor 22/C. Tel.: +36 1 391-1400 Fax: +36 1 391-1410 ugyfelszolgalat@naih.hu www.naih.hu

Кто: Nemzeti Adatvédelmi és Információszabadság Hatóság (Венгрия)

Кого: неизвестная компания

Когда: 2019.12

За что: нарушение ст. 5, 6 GDPR

Как: штраф €1,500

Причина: работодатель продолжал обработку и поиск писем в архиве корпоративной электронной почты работника, в которых содержалась личная переписка работника, после увольнения работника без правового основания. Работодатель не принял надлежащие организационные и технические меры для обеспечения безопасного для персональных данных поиска документов в архиве электронной почты, а также не проинформировал о таком процессе субъектов.

https://www.naih.hu/files/NAIH-2019-51-hatarozat.pdf

Штраф за незаконную автоматическую пересылку электронной корреспонденции работника

Datatilsynet

Lover og regler / Sentrale avgjørelser / 2021

Får gebyr for videresending av e-post

Datatilsynet har ilagt en virksomhet et overtredelsesgebyr på 400 000 kroner for ulovlig automatisk videresending av en ansatts e-postkasse.

Bakgrunn for saken er en klage fra en arbeidstaker som opplevde at arbeidsgiveren hadde aktivert automatisk videresending av vedkommende sin e-postkasse i virksomheten.

Mangler rettslig grunnlag

Den automatiske videresendingen ble aktivert i forbindelse med arbeidstakerens sykefravær, og varte i over en måned. Etter å ha undersøkt saken nærmere har Datatilsynet konkludert med at videresendingen har skjedd i strid med reglene i forskriften om arbeidsgivers innsyn i e-postkasse og annet elektronisk materiale, samt personvernforordningens krav til rettslig grunnlag, informasjon til *den registrerte* og plikten til å vurdere arbeidstakerens protest.

På bakgrunn av dette har Datatilsynet fattet vedtak om at virksomheten må utbedre de skriftlige rutinene for innsyn i e-postkasse, samt et pålegg om å betale et overtredelsesgebyr på 400 000 kroner for den ulovlige videresendingen.

Virksomhetens navn er unntatt offentlighet for å skjerme klagers identitet. Virksomheten har påklaget vedtaket.

Kontaktperson

Ole Martin Moe
juridisk rådgiver

Kontor: (+47) 22 39 69 59
E-post: omm@datatilsynet.no

Publisert: 12.01.2021

Кто: Datatilsynet (Норвегия)

Кого: неназванная компания

Когда: 2021.01

За что: нарушение ст. 5, 6 GDPR

Как: возможный штраф €38,600

Причина: расследование было инициировано по жалобе работника, который узнал, что работодатель активировал автоматическую пересылку сообщений из служебной электронной почты этого работника. Пересылка проводилась в связи с подозрениями в отношении обоснованности ухода сотрудника на больничный и длилась более месяца. По мнению надзорного органа, это ущемило права работника на защиту приватности. Компания обжаловала вынесенное решение в суде.

https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/far-gebyr-for-videresending-av-e-post/

Благодарю за ваше внимание