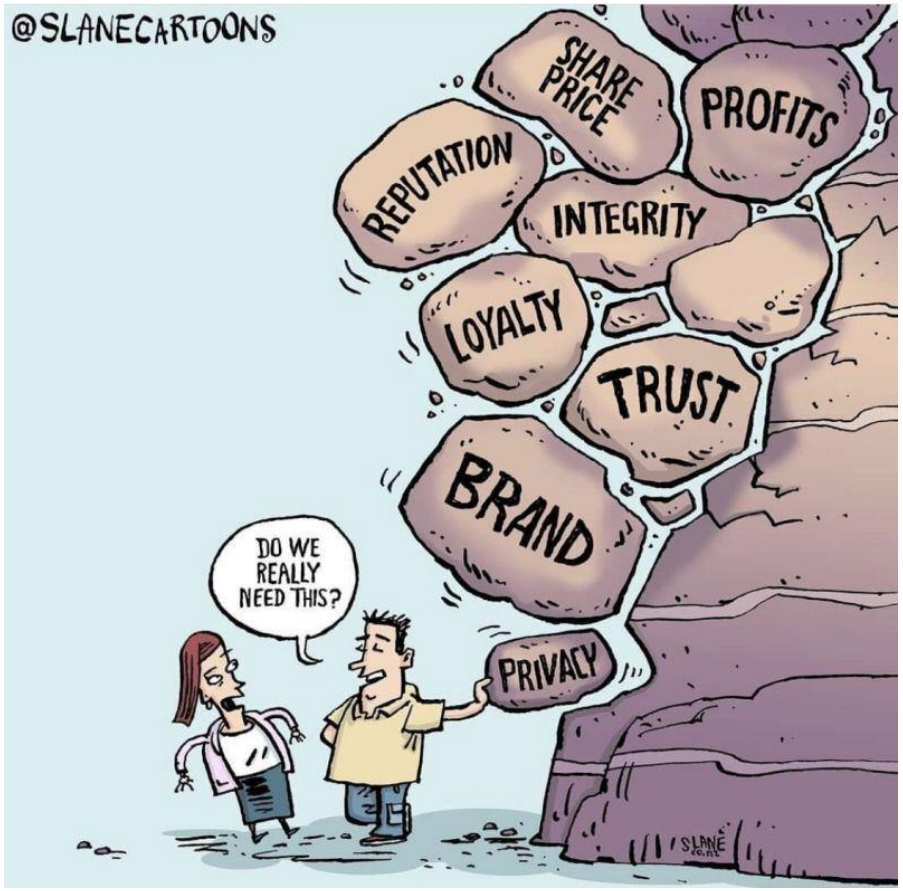
**Соблюдение требований законодательства о ПД | Алексей Мунтян**
**при внедрении/использовании DLP |** *Редакция от 05.10.2022*



**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

# *Благодарю за ваше внимание*


**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**