RACI матрица

	Направление деятельности	Менеджмент / ГД	ИБ	ИТ	Юристы	DPO	PR	HR	Маркетинг
1	Обнаружение								
1.1	Каналы и средства для получения уведомлений DPO об инциденте	-	R	R	R	A	-	R	R
1.2	Эскалация и старт реагирования рабочей группы	R	R	C	I	A	I	I	-
1.3	Первичная классификация	I	R	C	C	A	-	-	-
2	Первичное реагирование								
2.1	Локализация утечки	I	A	R	-	C	-	-	-
2.2	Устранение причины	I	A	R	-	C	-	-	-
2.3	Сбор ИБ артефактов	I	R	R	C	A	-	-	-
2.4	Сбор legal и комплаенс артефактов	I	I	I	R	A	-	-	-
2.5	Внутреннее расследование, а также внешнее расследование при необходимости	I	A, R	R	C	R	-	-	-
2.6	Оценка масштаба	I	R	C	R	A	-	-	-
2.7	Оценка рисков субъектов	I	R	-	R	A	-	-	-
2.8	Решение об уведомлении	I	C	-	R	A	I	I	-
3	Коммуникации с контрагентами								
3.1	Расторжение договора с контрагентом, допустившим утечку	I	R	R	R	A	-	-	-
3.2	Получение сведений об утечке, обмен контактами для оперативного взаимодействия	I	R	R	R	A	-	-	-

	Направление деятельности	Менеджмент / ГД	ИБ	ИТ	Юристы	DPO	PR	HR	Маркетинг
4	Регуляторные активности								
4.1	Уведомление РКН	I	C	-	I	A, R	-	-	-
4.2	Повторное уведомление	I	C	-	I	A, R	-	-	-
4.3	Подготовка позиции для проверки или адм. расследования	I	C	-	C	A, R	-	-	-
4.4	Заявление в полицию	I	C	-	A, R	C	-	-	-
5	Коммуникации								
5.1	Подготовка коммуникационной стратегии	A	C	-	C	C	R	R	C
5.2	Уведомление субъектов	I	C	-	R	A	R	R	C
5.3	Усиление контроля за приемом обращений	I	C	-	R	A	R	R	-
5.4	Ведение журнала обращений и подготовка ответов субъектам	I	C	-	R	A, R	R	R	-
5.5	Компенсации субъектам	A	-	-	C	C	C	-	-
5.6	Мониторинг утечек и дампов данных	I	R	R	-	A	-	-	-
5.7	Требования об удалении опубликованных дапмов	I	C	-	C	A, R	R	-	-
6	Пост-инцидент								
6.1	Обновление мер безопасности	I	A, R	R	-	I	-	-	-
6.2	Обучение сотрудников	I	R	C	C	A, R	-	R	-
6.3	Отчет об исправлении причин инцидента и мерах недопущения инцидентов в будущем	I	R	R	R	A	-	-	-

Ответственный (R):
- Лицо (лица), которое фактически выполняет задачу или деятельность.
- Они отвечают за выполнение задания или следят за тем, чтобы деятельность была выполнена.

Подотчетный (A):
- Лицо, обладающее правом принимать решения (вето) и обеспечивать выполнение задачи или деятельности.
- Этот человек несет полную ответственность за выполнение задания.

Консультирует (C):
- Лицо (лица), которое вносит свой вклад в выполнение задачи или деятельности.
- С ними советуются перед принятием решений и действий. Их отзывы и советы имеют решающее значение для успешного выполнения задания.

Информирован (I):
- Лицо (лица), которое информируется о ходе или результатах выполнения задачи или деятельности.
- Они получают информацию о решениях, результатах или изменениях, но не принимают непосредственного участия в выполнении задачи.

Инструкция для работников

Общие правила

- ☐ Не обсуждать инспектора или ход проверки в коридоре, зонах курения, лифтах и иных местах общего пользования
- ☐ Строго соблюдать сроки предоставления запрашиваемой информации, не откладывать на последний момент
- ☐ Если какие-то документы / сведения по запросу РКН отсутствуют – оперативно информировать об этом рабочую группу
- ☐ Не стесняться консультироваться с рабочей группой при подготовке ответа на запрос
- ☐ Оперативно информировать рабочую группу, если поступивший запрос РКН относится к другому подразделению или работнику
- ☐ Вести учет и хранить копии поступающих в свой адрес и направленных рабочей группе вопросов, писем, и документов
- ☐ Не взаимодействовать с РКН самостоятельно без полномочий, любые коммуникации с РКН осуществлять через рабочую группу, даже если инспектор требует быстрее или сейчас же
- ☐ Не комментировать работу других сотрудников, даже если об этом просит инспектор РКН
- ☐ Не рассказывать как было когда-то, если иное не согласовано с рабочей группой

Помещения и рабочие места

- ☐ Проверить документы, которые складируются в коробках, тумбах, шкафах и на подоконниках: документы, подлежащие хранению, переместить в запираемые на ключ шкафы, тумбы, сейфы
- ☐ Провести ревизию документов на столе и в кабинете: все распечатанные копии и документы, не подлежащие хранению, должны быть уничтожены или переданы в архив
- ☐ Убедиться, что документы, содержащие разные категории ПД и/или обрабатываемые в разных целях, хранятся отдельно
- ☐ Провести ревизию ПК: проверить рабочий стол, корзину, содержимое всех папок на наличие документов, хранение которых не предусмотрено ЛНА или срок хранения которых истек
- ☐ В период отсутствия (отпуск, больничный, командировка, а также совещаний, коротких перекуров или перерыва на обед) хранить документы в запираемых на ключ шкафах или тумбах
- ☐ Блокировать компьютер перед тем, как покинуть рабочее место
- ☐ Проверить замки на шкафах, тумбах и кабинетах, и наличие ключей от них, не оставлять ключи в замках
- ☐ Зачистить принтерные, места общего пользования, в том числе доски, экраны, стены от ПД (контакты, списки ДР работников и др.)

Обучение

- ☐ Пройти обучение по правилам работы с ПД и основам ИБ, чтобы разговаривать с инспектором на одном языке / ориентироваться
- ☐ Подготовиться (в том числе морально) к возможной демонстрации системы или интервью по своему направлению

Коммуникация при утечке

- ☐ Не обсуждать с инспектором и неуполномоченными работниками никакие инциденты, их причины и результаты расследования
- ☐ Не подтверждать факт утечки, переводить такие вопросы на DPO / рабочую группу
- ☐ Любое взаимодействие с инспектором осуществлять строго через рабочую группу и в присутствии рабочей группы / DPO

Процессы и документы

- ☐ Убедиться, что во вверенных процессах / продуктах используются актуальные / утвержденные DPO формы согласий / документов, CJM
- ☐ Проверить договоры с третьими лицами по своему направлению на наличие в них условий обработки ПД, при необходимости заключить дополнительные соглашения
- ☐ Изучить процессы обработки ПД в контуре своей ответственности на основании материалов от рабочей группы

Обучение

- ☐ Ограничиваться строго рамками поставленного вопроса: показывать и рассказывать только то, о чем спрашивает инспектор
- ☐ Не углубляться в детали, если инспектора не интересуют подробности или вопрос носит поверхностный характер, не выступать с инициативой провести демо или описать процесс
- ☐ Не передавать инспектору какие-либо документы, снимки экранов, выгрузки – это делает только рабочая группа
- ☐ Использовать нейтральные формулировки. Не говорить: «Не знаю», «У нас такого документа нет», «Кажется», «Наверное», «Это не реализовано» и т. д., отвечать – «Мы уточним и вернемся»
- ☐ Перед демонстрацией убедиться в наличии достаточных прав в системе, а также отключить излишние полномочия
- ☐ Не передавать мышь инспектору и не оставлять его одного с запущенной системой или доступом к документам на бумаге, не предлагать посмотреть систему самому
- ☐ По возможности проводить демонстрацию на синтетических данных и с «пустого» заранее подготовленного ИТ-командой ПК
- ☐ Немедленно информировать рабочую группу в случае получения каких-либо запросов напрямую от инспектора РКН

Порядок уведомления

72 часа с момента утечки *

ВСЕ РАБОТНИКИ

незамедлительно

Совершен / выявлен инцидент с ПД

Уведомить ИТ и ИБ

ПРИМЕРЫ ИНЦИДЕНТА

- Увидели пост в TG-канале про утечку
- Случайно направили ПД не тому лицу ВНЕ КОМПАНИИ
- Увидели в открытом доступе клиентскую базу в Интернете
- Получили письмо с угрозами от хакеров

ИТ / ИБ

Проверить информацию и провести расследование

Нужно сообщить об инциденте, даже если:

- (!) он произошел в отношении одного клиента/работника
- (!) вы думаете, что это утечка, но точно не уверены
- (!) вы думаете, что сообщение повлечет вашу ответственность за утечку (это не так)
- (!) это выходной / праздник / отпуск, и вы не хотите беспокоить коллег (у РКН нет выходных)

ЮРИСТЫ / МЕНЕДЖМЕНТ

Привлечь DPO в случае установления инцидента с ПД

Поддержка в подготовке уведомления

Согласование подачи уведомления

Направление уведомления

Таймлайн

- Фиксация результатов внутреннего расследования
- Принятие решения о подаче уведомления (с ИТ и ИБ)
- **24 часа:** подача уведомления об инциденте в РКН
- **72 часа:** подача уведомления о результатах расследования в РКН
- Дальнейшее взаимодействие с РКН

* Первое уведомление в течение 24 часов, второе – в течение 48 часов после первого уведомления

Артем Дмитриев
Управляющий партнер

artem.dmitriev@comply.ru
t.me/artydmitriev
+7 (961) 806 27 76

Comply.

Comply.ru
info@comply.ru
t.me/comply_ru
max.ru/comply