Construim
înCREDere!

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

ЗАКЛЮЧЕНИЕ

по проекту Закона о международном полицейском сотрудничестве

(проект одобрен Протокольным решением Правительства № 34 от 12 августа 2026 года; частично транспонирует Регламент (ЕС) 2024/982 — «Prüm II», Решение Совета 2008/615/ЈНА и Директиву (ЕС) 2023/977)

Кишинёв, 25 августа 2026 года

I. Предмет заключения

Гражданское движение «Construim Încredere» («Строим доверие») проанализировало проект Закона о международном полицейском сотрудничестве, посредством которого Республика Молдова устанавливает правовую основу для поиска и обмена полицейскими данными с государствами — членами Европейского союза, Европолом, ИНТЕРПОЛом и другими государствами, в том числе в автоматизированном режиме.

Проект касается особо чувствительных категорий данных — профилей ДНК, дактилоскопических данных, изображений лиц, данных о транспортных средствах, полицейских учётов, проездных документов, водительских удостоверений, а также данных о пропавших без вести лицах и неопознанных телах. Он знаменует переход от полицейского сотрудничества, основанного преимущественно на запросах и ответах, к модели, в рамках которой значительная часть проверок может осуществляться автоматически и практически мгновенно.

II. Общая позиция Движения

Движение поддерживает цель проекта. Приведение законодательства в соответствие с европейскими стандартами полицейского сотрудничества и транспонирование Регламента Prüm II являются необходимым шагом на пути европейской интеграции Республики Молдова и легитимным инструментом предупреждения и борьбы с трансграничной преступностью.

В то же время именно потому, что данный механизм предусматривает работу с наиболее чувствительными категориями персональных данных — биометрическими и генетическими, — уровень гарантий должен соответствовать уровню рисков. В нынешней редакции проект достаточно

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

подробно регулирует, «какие» данные обмениваются и «с кем», однако недостаточно регулирует, «как» обеспечиваются безопасность, контроль доступа и эффективная защита граждан. Существенная часть этих гарантий откладывается до принятия последующих подзаконных актов Правительства, что снижает предсказуемость закона и ослабляет парламентский и общественный контроль над вопросами, затрагивающими основные права человека.

Настоящее заключение носит конструктивный характер: оно признаёт положительные элементы проекта, указывает на существенные пробелы и предлагает конкретные решения по его совершенствованию до принятия.

III. Положительные элементы проекта

Проект содержит важные гарантии, которые необходимо сохранить и усилить:

● ограничение данных категориями, прямо предусмотренными законом, а также разграничение по категориям лиц — подозреваемый, обвиняемый, осуждённый, потерпевший, свидетель (ч. (2) ст. 2);

● принципы обмена информацией, включая законность, минимизацию данных, использование в индивидуальных случаях, подотчётность и контроль за дальнейшим распространением данных (ст. 4);

● ручное подтверждение квалифицированным персоналом любого совпадения («hit») до его дальнейшего использования (ч. (7) ст. 11, ч. (3) ст. 14, ч. (5) ст. 19);

● запрет на использование автоматизированного поиска по изображениям лиц для создания профилей, способных привести к дискриминации (ч. (3) ст. 19);

● проведение оценки воздействия на защиту данных (DPIA) и консультации с Национальным центром по защите персональных данных (CNPDCP) до подключения к Router/EPRIS (ч. (6) ст. 46);

● журналирование операций доступа к данным и обмена ими, а также контроль законности, осуществляемый CNPDCP (ст. 43, ч. (6) ст. 45);

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

● право лица на получение информации, исправление и удаление данных, подачу жалобы и получение компенсации (ст. 47).

IV. Существенные замечания

1. Чрезмерно широкие формулировки и предсказуемость закона

Сфера применения закона определена очень широко. Помимо обмена данными, проект допускает сотрудничество через ИНТЕРПОЛ, Европол, совместные группы, офицеров связи, совместные операции и «иные формы сотрудничества» (п. h) ч. (2) ст. 1, ч. (3) ст. 2). Используются открытые формулировки, такие как «не ограничиваясь ими» (например, п. 17 ст. 3 и ч. (4) ст. 6). Для органического закона, разрешающего автоматизированную обработку биометрических данных, подобные формулировки снижают предсказуемость и затрудняют контроль за фактическими пределами действия механизма. Рекомендуем прямо определить исчерпывающие рамки форм сотрудничества и исключить либо чётко ограничить открытые положения.

2. Чрезмерное делегирование ключевых гарантий Правительству

Значительное число элементов, имеющих определяющее значение для защиты прав, отнесено к регулированию нормативными актами Правительства: стандарты качества данных (ч. (5) ст. 10, ч. (2) ст. 13), структура референсного номера для изображений лиц (ч. (2) ст. 17), процедуры и гуманитарные случаи поиска (ч. (2) ст. 22), содержание запросов и сроки их исполнения (ч. (6) ст. 6), организация единого контактного пункта и национальных контактных пунктов (ч. (7) ст. 6), режим безопасности учётных систем (ч. (4) ст. 42) и другие вопросы. Гарантии, затрагивающие основные права, должны быть закреплены непосредственно в органическом законе, а не в подзаконных актах, чтобы обеспечить предсказуемость, парламентское обсуждение и общественный контроль.

3. Пробелы в сфере безопасности данных и управления доступом

Несмотря на то что проект неоднократно упоминает «шифрование и иные технические и организационные меры» (ч. (4) ст. 10, ч. (4) ст. 13, ч. (7) ст. 19 и др.), он не устанавливает проверяемый минимальный стандарт безопасности. Технико-правовой анализ выявляет следующие пробелы:

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

a) Не определён минимальный уровень безопасности (security baseline) для интеграций. Отсутствуют технические требования для Router, EPRIS, EUCARIS и INTERPOL, стандарты шифрования, требования по сегментации сети, а также по резервному копированию и аварийному восстановлению (backup/DR). Формула «шифрование + технические и организационные меры» не является полноценным baseline: каждый интегратор сможет реализовывать её по собственному усмотрению.

b) Отсутствует обязательная оценка безопасности перед вводом системы в эксплуатацию (go-live), отдельная от DPIA. Не предусмотрены моделирование угроз, тестирование уязвимостей, проверка go/no-go и формальное одобрение безопасности. DPIA (ч. (6) ст. 46) касается защиты персональных данных, а не зрелости системы информационной безопасности; ч. (7) ст. 46 возлагает на Агентство электронного управления «контроль межсистемного подключения», не устанавливая при этом процедуры оценки.

c) Недостаточно разработана модель управления идентификацией и доступом (IAM). Пункт d) ч. (5) ст. 51 и ч. (2) ст. 45 предусматривают права доступа, аутентификацию, прослеживаемость и списки уполномоченных лиц, однако проект не закрепляет: многофакторную аутентификацию (MFA), ролевую модель доступа (RBAC), принцип минимальных привилегий, разделение обязанностей (кто инициирует поиск и кто подтверждает «hit»), периодический пересмотр прав доступа с установленными сроками, отключение доступа при увольнении или переводе на другую должность, экстренный доступ («break-glass»), а также назначение единого ответственного за модель доступа. Закон допускает автоматизированный доступ к ДНК, дактилоскопическим данным, изображениям лиц и уголовным учётам, но не определяет, кто проектирует, реализует и контролирует систему доступа.

d) Отсутствует единая политика хранения и удаления данных. Сроки фрагментарны: 1 год (ч. (3) ст. 28), 3 года (ч. (4) ст. 43, ч. (5) ст. 45), 18 месяцев (ч. (7) ст. 45), «немедленное удаление» (ч. (5) ст. 46), а также ссылки на нормативные акты Правительства и национальное законодательство. Отсутствуют единая матрица сроков по категориям данных, правила для резервных копий и ложноположительных результатов, а также чёткая взаимосвязь между «немедленным удалением» данных и сохранением журналов.

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

e) Отсутствует операционная модель реагирования на инциденты (incident response). Части (6)–(7) ст. 9 предусматривают лишь ограничение последствий и уведомление партнёров. Не регламентированы классификация инцидентов по уровням критичности, внутренняя цепочка эскалации, роль ответственного за инцидент, сроки реагирования и восстановления, а также анализ после инцидента — элементы, имеющие критическое значение при утечке биометрических данных.

f) Недостаточная система мониторинга безопасности. Хранение журналов в течение трёх лет (ст. 43) и ежегодная проверка (ст. 48) представляют собой audit trail, но не полноценный мониторинг. Отсутствуют централизованная корреляция журналов (SIEM), оповещение в режиме реального времени, обнаружение аномалий (массовые запросы, доступ в нерабочее время, аномальные выгрузки данных) и неизменяемые журналы. Массовый несанкционированный доступ может остаться незамеченным до проведения ежегодной проверки.

g) Безопасность цепочки поставок и третьих лиц не урегулирована. Отсутствуют требования и положения о безопасности в отношении eu-LISA, INTERPOL и услуг хостинга, а также механизмы контроля субпроцессоров.

h) Отсутствует управление уязвимостями и обновлениями. Не предусмотрены сроки установки исправлений безопасности, периодичность сканирования уязвимостей и обязательное тестирование безопасности после внесения изменений.

i) Отсутствует матрица ответственности в сфере безопасности. Нет схемы «система → владелец → администратор → аудитор → ответственный за инцидент», а также не назначен единый ответственный за общий уровень безопасности всего механизма.

4. Недостаточные гарантии для граждан

Хотя ст. 47 признаёт права на получение информации, исправление и удаление данных, подачу жалобы и получение компенсации, их эффективная реализация зависит от процедур, которые должны быть установлены позднее. В условиях автоматизированного трансграничного механизма, где ошибка может быстро распространиться между несколькими государствами, гражданину необходим ясный, доступный и

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

быстрый механизм правовой защиты в случае, если переданная о нём информация является неверной или используется неправомерно. Рекомендуем прямо закрепить в законе механизм исправления ситуации и обязанность уведомлять соответствующее лицо в строго установленные сроки.

5. Неясность распределения контрольных полномочий

Проект возлагает контроль безопасности межсистемного подключения на Агентство электронного управления (ч. (7) ст. 46), тогда как CNPDCP осуществляет контроль законности обработки данных (ч. (6) ст. 45, ст. 46), а значительные киберинциденты относятся к компетенции органа в сфере кибербезопасности. Сосуществование этих компетенций без их чёткого разграничения может привести как к дублированию функций, так и к образованию зон, за которые фактически никто не отвечает. Рекомендуем прямо разграничить функции: CNPDCP — законность обработки данных; Агентство электронного управления — техническая безопасность межсистемного подключения; орган в сфере кибербезопасности — киберинциденты; единый контактный пункт — операционное управление и модель доступа.

V. Вопросы автору проекта и Парламенту

1. Какие конкретные гарантии предусмотрены для защиты персональных данных граждан?
2. Кто контролирует и проверяет законность обмена информацией с иностранными органами власти?
3. Каким механизмом правовой защиты может воспользоваться гражданин, если переданная о нём информация является неверной или используется неправомерно?
4. На какое учреждение, подведомственное Министерству внутренних дел, возлагается исполнение данного проекта закона?

Проект частично отвечает на четвёртый вопрос: исполнение возлагается на специализированное подразделение по международному полицейскому сотрудничеству, подведомственное Генеральному инспекторату полиции, — единый контактный пункт, включающий Национальное центральное бюро ИНТЕРПОЛ, Национальный контактный пункт ЕВРОПОЛ и Национальное бюро SIRENE (ст. 6). При этом остаётся неясным, кто

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

несёт единую ответственность за безопасность и управление доступом на уровне всего механизма.

VI. Рекомендации

Для того чтобы механизм был одновременно эффективным, безопасным и заслуживающим доверия граждан, Движение рекомендует до принятия проекта дополнить его следующими положениями:

1. обязательный минимальный стандарт безопасности (baseline) для всех интеграций, закреплённый в законе либо посредством ссылки на проверяемый нормативный акт;
2. обязательная оценка безопасности до подключения и ввода в эксплуатацию (go-live), отдельная от DPIA, с формальным одобрением безопасности;
3. чёткая модель IAM — MFA, RBAC, принцип минимальных привилегий, разделение обязанностей, периодический пересмотр прав доступа с установленными сроками, отключение доступа после прекращения исполнения функций, экстренный доступ и назначение ответственного лица;
4. единая матрица сроков хранения и удаления по категориям данных, включая правила для резервных копий и ложноположительных результатов;
5. модель реагирования на инциденты, предусматривающая классификацию, цепочку эскалации, сроки и анализ после инцидента;
6. непрерывный мониторинг безопасности — корреляция журналов посредством SIEM, оповещение, выявление аномалий и неизменяемые журналы;
7. требования по безопасности для третьих лиц и цепочки поставок, включая договорные положения и право на проведение аудита;
8. управление уязвимостями и обновлениями с установленными сроками и тестированием после внесения изменений;
9. матрица ответственности в сфере безопасности и назначение единого ответственного за общий уровень безопасности механизма;
10. прямое разграничение контрольных полномочий между CNPDCP, Агентством электронного управления, органом в сфере кибербезопасности и единым контактным пунктом;

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

11. ясный и оперативный механизм правовой защиты для гражданина, пострадавшего вследствие неверных данных или их неправомерного использования;
12. закрепление непосредственно в органическом законе ключевых гарантий, которые в нынешней редакции делегированы Правительству.

VII. Заключение

Гражданское движение «Construim Încredere» («Строим доверие») приветствует намерение привести законодательство Республики Молдова в соответствие с европейскими стандартами полицейского сотрудничества и поддерживает принятие современной нормативно-правовой базы в данной области. Вместе с тем мы призываем дополнить проект перечисленными выше гарантиями безопасности, механизмами управления доступом и защиты граждан, чтобы расширенные полномочия по обмену чувствительными данными сопровождались соразмерно эффективным контролем. Только безопасный и прозрачный механизм может заслужить доверие граждан — доверие, которое мы взяли на себя обязательство строить.

Гражданское движение «Construim Încredere» («Строим доверие»)

Кишинёв, 25 августа 2026 года