ГАНЗОВСКА Леа[1]

УДК: 343.45:[336.734:004.738.5(497.7)
343.45:340.137(497.7:4-672ЕУ)

ЗЛОУПОТРЕБА НА ЛИЧНИТЕ ПОДАТОЦИ ПРИ ОНЛАЈНКРЕДИТИРАЊЕ: ПРАВНА РАМКА, ПРАКТИЧНИ ПРЕДИЗВИЦИ И НАСОКИ ЗА УНАПРЕДУВАЊЕ

Апстракт
Во современата финансиска пракса, онлајн кредитирањето е просперитетен, но истовремено ризичен сегмент што овозможува брз пристап до средства. Сепак, ширењето на брзите онлајн кредити е проследено со растечки случаи на злоупотреба на лични податоци, каде криминални групи користат украдени или лажно прибавени идентитети за да одобрат и повлечат кредити на несреќни жртви. Овој академски труд ги анализира правната рамка (европска и македонска) која регулира заштитата на личните податоци и кредитирањето, презентира практични предизвици и конкретни случаи на злоупотреба, како и насоки за унапредување на системот.
Истражувањето користи примери од Македонија и пошироко во Европската Унија во изминатите пет години. Клучните заклучоци укажуваат на потребата за заострување на регулативата, подобрување на техничките и организациските мерки за заштита, и едукација на јавноста за правилна заштита на личните податоци при онлајн кредитирање.
***Клучни зборови**: лични податоци, онлајн кредитирање, брзи кредити, закон за заштита на лични податоци, злоупотреба, кривично дело, GDPR, препораки.*

GANZOVSKA Lea[2]

ABUSE OF PERSONAL DATA IN ONLINE LENDING: LEGAL FRAMEWORK, PRACTICAL CHALLENGES AND DIRECTIONS FOR IMPROVEMENT

Abstract: In modern financial practice, online lending is a thriving but at the same time risky segment that provides quick access to funds. However, the spread of fast online loans is accompanied by growing cases of personal data abuse, where criminal groups use stolen or fraudulently obtained identities to approve and withdraw loans from unfortunate victims. This academic paper analyzes the legal framework (European and Macedonian) that regulates the protection of personal data and lending, presents practical challenges and specific cases of abuse, as well as guidelines for improving the system. The research uses examples from Macedonia and the wider European Union in the past five years. Key conclusions indicate the need for tightening regulation, improving technical and organizational protection measures, and educating the public about the proper protection of personal data in online lending.
***Keywords:** personal data, online lending, fast loans, personal data protection law, abuse, criminal offense, GDPR, recommendations.*

Вовед

Личните податоци претставуваат особено чувствителен ресурс во дигиталниот свет, а нивната заштита е основно човеково право предвидено со меѓународни и национални регулативи. Со дигитализацијата на финансиските услуги и појавата на онлајн кредитните платформи, потребата од собирање и обработка на лични информации стана неизбежна во процесот на одобрување кредити. Ова отвора ризик од злоупотреба: доколку системите за верификација на идентитет се небезбедни или неадекватни, измамниците можат да користат украдени податоци за добивање кредити на туѓо име. Во македонската пракса се забележани случаи каде жртвите, вклучувајќи и лица со посебни потреби, остануваат со долгови што никогаш не ги подигале. Овој труд цели да ги истражи трендовите и проблемите во

[1]М-р; Докторанд на Правен факултет, Универзитет „Гоце Делчев“ – Штип; ganzovska19@gmail.com; lea.3077@student.ugd.edu.mk;
[2]LLM; PhD student at Faculty of Law, Goce Delcev University, Stip; ganzovska19@gmail.com; lea.3077@student.ugd.edu.mk

злоупотребата на лични податоци при онлајн кредитирање, да ги спореди европските и домашните регулативи, и да предложи насоки за унапредување на заштитните механизми.

1. Правна рамка за заштита на лични податоци и кредитирање согласно Европска регулатива

Во рамките на Европската Унија, Заштитата на лични податоци е уредена главно преку Општата регулатива за заштита на податоци (во понатамошниот текст GDPR) ((EU), 2016) која стапи на сила во мај 2018 година. GDPR налага принципи како ограничување на целите на обработка, минимизација на собирани податоци, јасно известување до субјектот за тоа како ќе бидат користени податоците, како и обврска за обезбедување на безбедност при чување и пренос на податоците. Регулативата им дава на граѓаните права како што се пристап до своите податоци, корекција и бришење (правото „да се заборави“), но и надомест на штета при повреда. Во контекст на онлајн кредитирање, GDPR го следи и принципот за „прозрачност“ – финансиските институции мора јасно да наведат зошто и како користат лични податоци за кредитна оценка.
Наредни чекори во ЕУ се развивањето на дигиталната евалуација на идентитет (eIDAS 2) и регулативи за геометриска заштита, кои дополнително ќе влијаат на начинот на електронско идентификување на клиентите.
Согласно Регулативата за заштита на лични податоци позната како *Општа регулатива за заштита на податоци* (GDPR) претставува клучен законски инструмент на Европската Унија со кој се уредува обработката на лични податоци. Овој правен акт има особено влијание врз финансискиот сектор, каде што прецизниот третман на чувствителни информации е императив, особено во процесите на кредитирање[3]. Кога зборуваме за GDPR постојат принципи кои применливи во кредитирањето, а финансиските институции подлежат на обврски според неколку фундаментални принципи на GDPR:

- *Законитост, правичност и транспарентност*: Обработката на лични податоци мора да биде заснована на јасна законска основа, а клиентите мора да бидат информирани за начинот и целта на обработката (GDPR, Article 5)[4].
- *Минималност на податоците*: Институциите смеат да собираат само оние податоци кои се неопходни за конкретната цел – на пример, кредитна историја, финансиски приходи, и основни идентификациски информации (GDPR, Article 5).
- *Права на субјектот на податоци*: GDPR им гарантира на клиентите право на пристап, корекција, ограничување и бришење на нивните податоци, како и право на приговор (Commission, CERV Programme Projects 2023 Overview, 2023)

Со цел олеснување на имплементацијата на GDPR, особено кај мали и средни претпријатија (МСП), Европската комисија преку програмата *Citizens, Equality, Rights and Values (CERV)* финансира повеќе проекти (Commission, CERV Programme Projects 2023 Overview, 2023):
Во Австрија развиена е алатка за самооценување на GDPR усогласеност кај МСП, во Кипар имплементира дигитална платформа за едукација и тестирање на организациските практики (Cyprus Data Protection Office, 2023), во Германија обезбеди обуки за предавачи кои работат со млади лица со цел разбирање на приватноста, Словенија поддржа програма за подигнување на свеста кај деца и родители за важноста на заштитата на личните податоци (Slovenian Information Commissioner, 2023).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (Commission, Data Protection in the EU, n.d.; (EU), 2016)

[4] *Article 5*/Principles relating to processing of personal data/1. Personal data shall be:
(a)processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

Општата регулатива за заштита на личните податоци (GDPR), донесена од Европскиот парламент и Советот во 2016 година, претставува суштински инструмент за заштита на личната приватност на поединци во Европската Унија.
Во доменот на финансиското кредитирање, оваа регулатива воспоставува фундаментални принципи кои обезбедуваат транспарентност, одговорност и интегритет во обработката на личните податоци, тоа се: законитост, правичност и транспарентност каде што обработката на податоци мора да има правна основа како што е договорна обврска, законски мандат или легитимен интерес на контролорот (GDPR A. 5.–P.). Институциите задолжително мора да информираат клиентите за целта и начинот на обработка. На пример, при апликација за кредит, клиентот мора да знае кои податоци се собираат и за која цел. Како дел од фундаменталните принципи , се и ограничување на целта, каде што GDPR бара секоја обработка да биде врз основа на однапред дефинирана и легитимна цел (GDPR A. 5.–P.), а податоците собрани за кредитна евалуација не смеат да се користат за маркетинг, освен ако постои изречна согласност од клиентот. Исто така , фундаментален принцип е и минималност на податоците, односно само податоците кои се неопходни за исполнување на конкретната цел смеат да се прибираат (GDPR A. 5.–D.). На пример, барање за потрошувачки кредит не оправдува обработка на биометриски или здравствени податоци. Принципот на минималност на податоците, утврден во член 5(1)(c) од *Општата регулатива за заштита на личните податоци* (GDPR), претставува еден од темелите на етичката и законска обработка на лични податоци во Европската Унија. Според овој принцип, обработувачите смеат да прибираат и обработуваат само оние податоци кои се соодветни, релевантни и ограничени на она што е неопходно за исполнување на конкретната цел.
GDPR експлицитно бара од контролорите на податоци да избегнуваат прекумерно прибирање на информации. Тоа значи дека: не смеат да се бараат податоци „за секој случај“ и секоја категорија на податоци мора да има јасна функционална оправданост.
Овој принцип е тесно поврзан со другите GDPR принципи, како што се ограничување на целта и законитост.

Во Банкарскиот сектор, во процесот на кредитирање минималноста на податоците значи прибирање само на финансиски и идентификациски податоци релевантни за проценка на кредитна способност. Во овој дел Банката е потребно да направи избегнување на чувствителни категории (на пр. здравствени, етнички, биометриски) освен ако не се строго неопходни и законски оправдани (GDPR, Processing of special categories of personal data).

<u>Пример:</u> Банка не смее да бара информации за брачен статус или број на деца ако тие не влијаат директно врз кредитната проценка.

Како технички и организациски мерки, за да се обезбеди усогласеност со принципот на минималност, институциите треба да се спроведат проценка на влијание врз приватноста (DPIA) пред воведување нови форми на обработка и исто така да обезбедат обука на персоналот за свесност околу минималната обработка (АЗЛП, Нов правилник за лични податоци , 2025).

2. Македонска законодавна рамка

Со цел да се усогласи со европските стандарди за заштита на личните податоци, Република Северна Македонија го донесе новиот Закон за заштита на личните податоци во 2020 година. Овој закон претставува транспозиција на Регулативата (ЕУ) 2016/679 – Општа регулатива за заштита на податоци (GDPR), со што се овозможува хармонизација со правниот систем на Европската Унија.
Република Северна Македонија има усвоено Закон за заштита на лични податоци (СевернаМакедонија, 2020)кој е хармонизиран со GDPR. Овој закон ги пропишува принципите

на праведна обработка, дозволи за пренос на лични податоци, како и активностите на Дирекцијата за заштита на лични податоци како надлежен орган.
Покрај законодавството за податоци, криминалот поврзан со податоците е регулиран во *Кривичниот законик: така, злоупотребата на лични податоци е дефинирана како кривично дело (чл.149)*, кое може да резултира во казна затвор.
Слично, *подигањето кредит на туѓо име се третира како кривично дело (измама и кражба на идентитет), каде ИТ-техниките (компјутерска измама) и фалсификување лични исправа (член 378)* се во пракса чести соучесници.
Во финансискиот сектор, Народната банка на РСМ го регулира банкарското и кредитното работење, но многу „брзи заеми“ се издаваат од микрофинансиски друштва кои се надлежни на Министерството за финансии, а не на Централната Банка.
Тоа создава регулаторен вакуум – овие субјекти подлежат на деловно-законски контроли, но во случај на злоупотреба е неопходна реакција и од страна на органите за кривична правда и агенцијата за податоци.

Како основни принципи на GDPR и нивна имплементација во Македонското законодавство се: *Законитост, правичност и транспарентност* каде што обработката на лични податоци мора да биде законска, правична и транспарентна за субјектот на податоци, о*граничување на целта*: податоците се собираат за конкретни, експлицитни и легитимни цели и не смеат да се обработуваат понатаму на начин што не е во согласност со тие цели, м*инималност на податоци*: се обработуваат само оние податоци кои се соодветни, релевантни и ограничени на она што е неопходно, т*очност* на податоците мора да бидат точни и каде што е потребно да се ажурирани и како последен принцип е о*граничување на складирање на податоците* кои се чуваат во форма која овозможува идентификација на субјектите на податоци не подолго од потребното.

Национална имплементација на Македонскиот закон ги следи овие принципи и дополнително предвидува:

- Проценка на влијание врз приватноста (DPIA) за обработка со висок ризик.
- Назначување офицер за заштита на податоци (DPO) во јавни институции и поголеми организации.
- Санкции и инспекциски надзор од страна на Агенцијата за заштита на личните податоци (АЗЛП).
- Македонската законодавна рамка претставува значаен чекор кон европска интеграција и заштита на фундаменталните права на граѓаните. Усогласеноста со GDPR не е само формална обврска, туку и суштинска потреба за градење доверба во дигиталното општество.

Практични предизвици кои се потенцијал за измама при онлајн кредити

Онлајн кредитирањето, како современа алтернатива на традиционалните банкарски услуги, нуди брзина, достапност и минимална документација. Сепак, токму овие карактеристики отвораат простор за потенцијални злоупотреби, особено во контекст на лична приватност, финансиска безбедност и регулаторна контрола.
Онлајн кредитите („брзи кредити“) обично се одобруваат веднаш преку веб или мобилни апликации. Постапката речиси во целост се базира на внесување на лични податоци (име, адреса, МБР, серија број на лична карта, матичен број на личната карта итн.).
За разлика од традиционалните банки кои бараат проверка со документ на лице место, многу онлајн кредитори дозволуваат само слика/скенирани документи или банкарска верификација преку мали трансфери.
Така, измамниците може само со искористување на фотографии од изгубен личен документ, или со украдување на личните податоци од жртвата, да побараат кредит. Оваа леснотија ја создава главната практична ранливост: доколку се искористат туѓи податоци, личната картичка на жртвата дури и не мора да биде физички присутна. Полскиот пример дополнително појаснува дека во пракса за земање „брз кредит“ единствено е неопходно скенирање на лична карта, што го прави тој систем особено подложен на злоупотреби.

Онлајн кредитите често се одобруваат врз основа на електронски поднесени документи, што создава ризик од:

- Кражба на идентитет: Злоупотреба на лични податоци за аплицирање во име на друго лице (онлајн, 2025).
- Фалсификувани документи: Лажни потврди за приходи или адреса, особено кај небанкарски институции со слаби механизми за верификација.
- Недоволна транспарентност и скриени услови: Некои онлајн платформи не ги прикажуваат целосно условите за кредитирање, што води кон: *Скриени каматни стапки и трошоци* (кредити П. и., n.d.).*Автоматски продолжувања на договори* без експлицитна согласност.
- Недоволна регулаторна контрола: во Македонија, иако АЗЛП и Народната банка имаат надлежности, не сите онлајн кредитори се подложни на истите стандарди:
- Небанкарски институции често работат без лиценца или со ограничена супервизија (кредити L. –C.)
- Психолошки притисок и манипулативен маркетинг: онлајн кредитите често се рекламираат како „итни решенија“, што може да доведе до:
- Импулсивно задолжување кај ранливи категории (млади, невработени).
- Манипулативни реклами преку социјални мрежи и апликации (комисија, 2022)[5].
- Недоволна заштита на личните податоци: Иако GDPR е транспониран во македонското законодавство, не сите платформи го почитуваат: *недоволна енкрипција и заштита на податоци.*
- Продажба на кориснички информации на трети страни без согласност (АЗЛП, Годишен извештај за заштита на лични податоци, 2023, 2023).

Онлајн кредитирањето носи значителни предности, но и ризици кои бараат засилена регулаторна рамка, едукација на граѓаните и технички механизми за заштита. Потенцијалот за „имама“ не е само технички, туку и етички и социјален предизвик.

Скриени измамнички патеки

Скриен измамнички пакет се однесува на понуда или услуга која на прв поглед изгледа легитимно, но содржи скриени услови, манипулативни клаузули или лажни информации со цел да се измами корисникот (правници, https://myla.org.mk/49855/, н.д.). Овие пакети често се промовираат преку:

- Фалсификувани веб-страници кои имитираат банки или финансиски институции.
- Е-пошта или СМС пораки со итен тон („вашата сметка ќе биде блокирана“).
- Лажни наградни игри или „ексклузивни понуди“ кои бараат внес на лични податоци (https://izbiram.mk/, н.д.).

Криминалните мрежи често комбинираат кражба на податоци со социјален инженеринг. Во еден новинарски приказ на хумани жртви во Македонија, еден човек со церебрална парализа бил измамен преку социјални медиуми: му било наложено да ја слика личната карта и трансакциската сметка „за да прати пари од Америка“. Всушност, преку таа фотографија измамникот подигнал кредит на негово име. Родителите веднаш го платиле првиот кредит (40.000 денари) за да не „расне“ со камати, но наскоро се појавиле и други кредити од трети страни. На крајот, секојдневно непознати измамници ги вовлекувале во долгови, оставувајќи ги родители и детето безизлезно должни. Овој случај илустрира дека криминалците користат физички уценувачки техники (изневера) за да добијат пристап до податоците, а потоа користат слоеви од легитимни финансиски процедури (компаниите, правните системи) да ги реализираат

[5] (комисија, 2022)

злонамерните цели. Слични организирани измами беа евидентирани од Обвинителството во Скопје, каде обвинети се 43 лица за „компјутерска измама, фалсификување исправа и злоупотреба на лични податоци“ при брзи заеми.
Криминалната група систематски „креирала лажни јавни исправи (лични карти) и компјутерски впишувала туѓи податоци во информацискиот систем на кредитни компании“. Членови од групата дури фалсификувале евиденција за вработување на невработени лица, за да ги прикажат како погодни за кредит, и ги користеле податоците од Фондот за здравствено осигурување преку официјален службеник како помагач
На тој начин, мултиплицирале лажни кредити и ги повлекувале парите, со што оштетиле неколку десетици граѓани и кредитни здруженија. Вкупно, каматите нелегално „наплатени“ надминуваат милионски износи.

Исто така измамничките пакети функционираат преку неколку механизми:

- Фишинг: Корисникот е наведуван да внесе чувствителни информации преку лажна форма или линк (правници, myla.org.mk, н.д.).
- Смишинг: Слично на фишинг, но преку СМС пораки кои тврдат дека „пакетот е задржан“ или „кредитот е одобрен“ (Тераса, 2024)[6].
- Малвер и Ransomware: Во некои случаи, корисникот презема „документи“ кои содржат малициозен софтвер што ги шифрира податоците и бара откуп (правници, https://myla.org.mk/49855/, н.д.).

Импликации врз приватноста и безбедноста
Овие пакети често водат кон:

- Кражба на идентитет: Со доволно прибрани податоци, измамниците можат да аплицираат за кредити во име на жртвата.
- Финансиска штета: Непланирани задолжувања, неовластени трансакции и губење на средства.
- Правни последици: Жртвите може да се соочат со правни проблеми поради активности извршени во нивно име (Commission, Data Protection in the EU, н.д.).

Сепак постои превенција и регулаторни мерки кои се задолжителни, а тие се: едукација на граѓаните каде што преку кампањи ќе се препознавање кои се измамнички пораки и понуди, техничка заштита кои се составени од Антивирусни програми, двофакторска автентикација,енкрипција и регулаторна интервенција каде Националните тела како АЗЛП и Народната банка мора да следат и санкционираат нелегитимни платформи (АЗЛП, Годишен извештај за заштита на лични податоци, 2023, 2023).

Скриените измамнички пакети претставуваат сериозна закана за дигиталната безбедност и довербата во онлајн кредитирањето. Превенцијата бара мултидисциплинарен пристап: технички, правен и едукативен. Само преку соработка меѓу институциите и граѓаните може да се намали ризикот од вакви злоупотреби.

Технички и организациски слабости
Брзото кредитирање, како форма на финансиска услуга достапна преку интернет, носи значителни предности за граѓаните, но истовремено отвора простор за злоупотреба на лични податоци. Во контекст на дигиталната трансформација, техничките и организациските слабости кај финансиските друштва кои нудат брзи кредити се покажуваат како критични точки за нарушување на приватноста и безбедноста на корисниците.

Технички слабости
Во делот на техничките слабости недоволна енкрипција и заштита на податоци, многу платформи за брзи кредити не применуваат соодветни криптографски протоколи за заштита на личните податоци при нивно пренесување и складирање (АЗЛП, Водич за технички и

[6] (Тераса, 2024) Што е Смишинг и како да се заштитите од оваа закана

организациски мерски, 2024). Ова овозможува потенцијален пристап од трети лица, особено при користење на јавни мрежи.
Исто така слаба автентикација и пристап како недостаток на двофакторска автентикација (2FA) и слаби лозинки овозможуваат лесен пристап до кориснички профили, што може да доведе до кражба на идентитет и аплицирање за кредит во име на друго лице (ФАКТОР.МК, 2022).
Некои институции не применуваат политики за безбедно користење на мобилни телефони и USB уреди, што овозможува неовластено копирање или губење на чувствителни информации (АЗЛП, https://e-ucilnica.azlp.mk/, 2023).

Организациски слабости
Во делот на организациски слабости , најмногу акцент е поставен на недоволна едукација на персоналот.Тоа значи дека вработените често немаат доволно знаење за обработка на лични податоци, што води кон ненамерни повреди или злоупотреби (АЗЛП, Годишен извештај за заштита на лични податоци, 2023, 2023). Исто така како дел од оргабизациските слабости се и недефинирани интерни политики кои многу финансиски друштва немаат јасно дефинирани политики за пристап, чување и уништување на лични податоци, што создава хаос во управувањето со информациите (СевернаМакедонија, 2020). Оттука се провлекува и недоволна супервизија и ревизија, односно отсуството на редовни ревизии и контроли од страна на офицери за заштита на податоци (DPO) доведува до неусогласеност со законските обврски и зголемен ризик од злоупотреба.

3. Последици и препораки за соодветна заштита на личните податоци
Злоупотребата на лични податоци кај брзите кредити може да резултира со кражба на идентитет,финансиска штета, правни последици за жртвите. Во ваков случај, најмногу се препорачува да се направи спроведување на проценка на влијание врз приватноста (DPIA), имплементација на технички мерки како криптирање, логирање и резервни копии, усвојување на организациски мерки како обука, политики и интерни ревизии.
Овие случаи ја нагласуваат потребата од посилни механизми за идентификација,безбедносни стандарди, како и двофакторска автентикација и криптографија, каде што претставуваат „офанзивно“ таргетирање на безбедноста на податоците, но голем дел од „брзите кредитори“ (особено помалите небанкарски фирми) не применуваат доверлив процес на верификација.
Во Македонија, наведената законска измена на Правилникот за кредитен ризик го воведе барањето за физичко присуство на побарувачот при одобрување на „брз кредит“. Оваа мерка директно реагира на недостатокот откриен во претходните злоупотреби: законот сега налага дека електронските апликации само не се дозволени без лична проверка на клиентот. Тоа е примарна регулаторна интервенција која го елиминира сценариото на кредитирање само врз основа на фотографија од лична карта.
Од технички аспект, уште не се ефикасно искористени можности како национални дигитални идентитети или интегрирани државни системи за проверка, кои би можеле да се поврзат со кредитните апликации за аутоматска верификација. На пример, проверка на МБР, адреса и статус на осигурување (со дозвола на граѓанинот) би го оневозможила брзото „животно“ на лажните записи.
Дополнително, законодавецот мора да ги охрабри и финансиските друштва сами да воведат строги ИТ-мерки: пишани политики за заштита на лични податоци, обука на вработените, и планови за брз одговор на инциденти.

4.Едукација, јавна свест, препораки и насоки за унапредување
Во дигиталната ера, личните податоци се трансформираа во вредна валута, а нивната злоупотреба претставува сериозна закана за индивидуалната приватност и безбедност. *Едукацијата и јавната свест* се клучни алатки за превенција од злоупотреба, особено во контексти каде што граѓаните се изложени на ризици преку интернет, мобилни апликации и финансиски услуги.

Граѓаните често не знаат дека токму преку социјалните мрежи „хранат“ свои податоци кои потоа можат да се злоупотребат. Постојат и измамнички кампањи каде лажни реклами ветуваат лесни кредити за тргување или инвестиции, барајќи податоци и уплатници.
За потребите на ова истражување, анализата од Полска препорачува корисниците да не ги споделуваат деталите од личните документи на непознати страници и да користат сигурни канали за аплицирање. Истиот извор ги наведува потребните чекори кога се сомневаат на измама – побарување извештај од кредитни бироа и блокирање на лична карта. Сепак, не сите засегнати лица се информирани за овие алатки, а понекогаш финансиските субјекти не соработуваат лесно со бироата. Затоа, едукацијата на јавноста и промоција на мониторинг (на пр. преку БИРО, НЕБ или Инспекторатот за лични податоци) може да поминат како превентивни мерки.

Значењето на едукацијата е тоа што вклучување на теми за заштита на лични податоци во наставните програми, особено во средните училишта, овозможува рано стекнување на дигитална писменост и критичко размислување кај младите (ДЗЛП, 2015).
Организации како Центарот за правни истражувања и анализи (ЦПИА) и Македонското здружение на млади правници (МЗМП) организираат интерактивни работилници за ученици, каде се обработуваат реални случаи на злоупотреба и се нудат практични совети за заштита (ЦИПА, 2025). Кога би зборувале за Јавните институции тие имаат обврска да обучуваат своите вработени за правилна обработка на лични податоци, согласно Законот за заштита на личните податоци (РСМ С. в., 2020/2021)

Во горниот дел од текстот, спомнав за јавна свест и кампањи , тоа значи дека **к**ампањи за информирање се проекти како „Час по приватност“ и „Ефикасна правда за заштита на основните слободи“ имаат за цел да ја подигнат свеста кај граѓаните преку медиуми, социјални мрежи и јавни настани (правници, https://myla.org.mk/49855/, н.д.)
Исто така како најважна точка за едукацијата на малолетни лица , е улога на родителите каде што истражувањата покажуваат дека 60% од родителите сметаат дека тие самите треба да имаат водечка улога во едукацијата на децата за приватност на интернет.

Стратегијата за заштита на личните податоци 2025–2030 ја нагласува потребата од развој на култура на приватност преку континуирана едукација и вклучување на граѓаните во процесите на одлучување (АЗЛП, Стратегија за спроведување на правото за заштита на личните податоци во РСМ, /).

Како дел од едукацијата и јавната свест се и *препораките* кои се поврзани со воведување на предмет „Дигитална етика и приватност“ во основното и средното образование, поддршка на граѓански организации кои работат на едукација, спроведување на национални кампањи за подигнување на свеста како и обука на медиумите за етичко известување при случаи на злоупотреба.

Исто така насоките за унапредување на заштитата на личните податоци при онлајн кредитирање се предлагаат неколку мерки:

Засилување на идентификацијата: Примена на стандарди како KYC (Know Your Customer) и SCA (Strong Customer Authentication) барани со PSD2 и националните регулативи, така што кредиторите ќе мора да користат дво/мултифакторски системи (автентикациски мобилни потврди, електронски потписи и биометриска верификација) за одобрување нов клиент.
Интеграција со државни регистри: Користење на јавни бази (пописи, фондови) за проверка на статус и адреса, со автоматска размена на податоци помеѓу Министерствата и Банкарскиот систем. На пример, со врска со Регистарот за поединечни платежни сметки (FPS), се прави верификација на сопственикот на трансакциската сметка при апликација за кредит.
Законски измени и контрола: Должност за регистрирање на сите кредитни посредници и микрофинансиери, како и утврдување обврска за редовни ИТ-ревизии (скоро како во PSD2 за финтек субјекти). Додатно, ангажирање на надзорот на Дирекцијата за заштита на лични

податоци кон следење на задолженијата на кредиторите и креирање механизам за брзо реагирање при пријавена злоупотреба.
Механизми за жртви: Оформување на ефикасен систем за пријавување измама: евентуално национална платформа каде граѓаните можат да сигнализираат злоупотреба и да добијат правна помош (од правобранителство или адвокатски комори). Ова може да се поврзе и со опцијата за блокада на кредити преку БИРО (како се прави во Полска) – блокирање на идентитет во кредитни регистри.
Едукација: Регуларни информирање преку кампањи за заштита на лични податоци, алати за проверка, и ограничувања на споделување на чувствителни информации. Банки, здруженија и НВО можат да изработат бецови за кориснички-свесна апропријација (на пример „Nikogash ne gi dadete broevite od kartata“).

Во Македонија, воведувањето на правилникот за физичко присуство веќе е чекор кон ограничување на ризикот. За континуитет, Владата и Министерството за финансии можат да тестираат пилот-проекти за алтернативна идентификација: на пример, видео верификација преку мобилен телефон или соработка со мобилни оператори за сигурна аутентификација. Во меѓувреме, предлозите за измени на Кривичниот законик би можеле да предвидат повисоки казни за злоупотреба на податоци и забрзана постапка за ваквите измами, со цел криминалците да бидат отстрани од пазарот побрзо.

Во рамките на ЕУ, повеќето земји се соочуваат со слични предизвици како што покажуваат извештаите на Европол и ЕБА покажуваат зголемен интерес на организиран криминал во кражба на податоци.
Затоа, се препорачува меѓународна соработка (вклучувајќи европски органи како CEPOL и Europol) за размена на информации за мрежи кои издаваат нелегални онлајн кредити преку платформи и мрежи за перење пари. Спроведување на добри практики од други земји, како регистрирање на крајните кредитни корисници и стриктна проверка при онлајн аплицирање во Шведска или Германија, може да се приспособи и во локална средина.

Пример 1:

Во април 2025 година, јавноста во Северна Македонија беше потресена од откритието на организирана криминална група која со злоупотреба на лични податоци, фалсификување исправи и компјутерски измами, незаконски прибавила над три милиони денари преку брзи кредити. Овој случај претставува конкретен пример за техничките и организациските слабости во системите за обработка на лични податоци кај финансиските друштва.

Опис на случајот

- Механизам на измамата

Групата започнала со активности во јули 2022 година, користејќи туѓи лични податоци без согласност од граѓаните. Преку фалсификувани јавни исправи и електронски потписи, тие аплицирале за брзи кредити во десетина различни кредитни друштва, прикажувајќи ги жртвите како кредитоспособни лица (DW, 2025).

- Вклученост на службени лица

Во шемата бил вклучен и вработен во Фондот за здравствено осигурување, кој преку својот службен компјутер обезбедувал ЕЗБО број (единствен здравствен број) за жртвите, овозможувајќи пристап до нивните здравствени и лични податоци (РСМ Ј. о., 2025).

- Технички слабости

Недоволна заштита на информатичките системи на кредитните друштва, отсуство на механизми за проверка на идентитет, недоволна енкрипција и логирање на пристапи.

- Организациски слабости

Недостаток на интерни контроли и ревизии, недоволна обука на персоналот за заштита на лични податоци, отсуство на офицери за заштита на податоци во некои друштва.

- Последици

Финансиска штета за жртвите, кои биле обврзани да ги враќаат кредитите, правни постапки против 43 лица, од кои четворица се под истрага за фалсификување, злоупотреба и компјутерска измама, нарушување на довербата во дигиталните финансиски услуги.

- Препораки

Имплементација на двофакторска автентикација и биометриска идентификација,редовна обука на персоналот за обработка на лични податоци, воспоставување на офицери за заштита на податоци (DPO) и спроведување на проценка на влијание врз приватноста (DPIA) пред секоја нова услуга.

Заклучок

Злоупотребата на личните податоци во онлајн кредитирањето е сериозен безбедносен и социјален проблем во дигиталното општество. Анализата покажа дека иако постојат напори за заштита преку законодавството (на пр. хармонизиран PDPL со GDPR), во практиката често наидуваме на бели точки – посебно кај фирмите за брзи кредити. Регулаторните интервенции (како физичкото присуство при одобрување кредит) и личните жалби на жртви упатуваат дека е потребна поголема координација меѓу државните органи и финансиските субјекти. За ревитализација на довербата во дигиталните кредити, неопходно е интегрирање на технички решенија (силна автентикација, верификација со државни регистри) и зголемена јавна свест. Следејќи ги европските насоки за борба против финансискиот криминал (како што European IOCTA 2025 ја дефинира кражбата на податоци како „важен извор“ на криминалната економија), Македонија треба да ги прилагоди своите пракси и казнени политики. Само со севкупен пристап – законски, технички и образовен – може да се минимизира ризикот од злоупотреба и да се обезбеди сигурно онлајн кредитирање за граѓаните.

Користена литература

1. Directive 95/46/EC (General Data Protection Regulation) http://data.europa.eu/eli/reg/2016/679/oj
2. *Article 5/*Principles relating to processing of personal data/1.
3. (EU), R. (2016). *General Data Protection Regulation)*. Повратено од http://data.europa.eu/eli/reg/2016/679/oj. (ОГРМ 42/20, 2. (n.d.).
4. Commission, E. (2023). CERV Programme Projects 2023 Overview.
5. Commission, E. (n.d.). *Data Protection in the EU*. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en
6. Cyprus Data Protection Office, 2. I. (2023).
7. DW. (2025, 4 10). *https://www.dw.com/mk/*. Retrieved from https://www.dw.com/mk/: https://www.dw.com/mk/razbiena-sema-so-brzi-krediti-kako-se-odvivala-izmamata/a-72197796
8. GDPR. (n.d.). Integrity and Confidentiality.
9. GDPR. (n.d.). Accuracy.
10. GDPR. (n.d.). Article 5.

11. GDPR. (n.d.). Processing of special categories of personal data. *Processing of special categories of personal data*, p. Article 9.
12. GDPR. (n.d.). Storage Limitation.
13. GDPR, A. 5. (n.d.).
14. GDPR, A. 5.–A. (n.d.).