Journal of Sustainable Development of Transport and Logistics
journal home page: https://jsdtl.sciview.net

Chiappetta, A., & Battaglia, A. (2018). The impact of privacy and cybersecurity on e-record: The PNR Directive Adoption and the impact of GDPR. *Journal of Sustainable Development of Transport and Logistics, 3*(3), 77-87. doi:10.14254/jsdtl.2018.3-3.6.

ISSN 2520-2979

The impact of privacy and cybersecurity on e-record: The PNR Directive Adoption and the impact of GDPR

Andrea Chiappetta [1], Andrea Battaglia [2]

[1]*Marconi International University,*
111 NE 1st street, Miami -33132 Florida, USA
PhD, Professor
[2]*ASPISEC,*
Piazzale Flaminio 19 – 00196 Rome, Italy
Security Policy Manager

Article history:

Received: September 15, 2018
1st Revision: October 5, 2018
Accepted: November 29, 2018

DOI:
10.14254/jsdtl.2018.3-3.6

Abstract: Digital transformation means radically change how we manage interaction with everything, including goods, persons and data flows. Cyberspace is by nature borderless and open to everybody, and any sensitive personal info passing through it should be appropriately managed to ensure the protection of the users' identity and other personal records. The Passenger Name Record (EU Directive **2016/681**) impacts for travellers, e-wallets for online shoppers, medical e-records for patients, etc., which may contain personal information provided by the users and collected by the service providers during the on-line transaction. While such records need to be shared for the smooth operation of the provided service, evidence shows that such sharing does not always respect the privacy of the data subjects. This paper address this challenge by proposing a comprehensive solution to safeguard and protect such on-line info and to preserve and protect the users' privacy (GDPR) in order to improve the cybersecurity aspects at EU level with a focus on transports and blockchain.

Keywords: blockchain, transport, general data protection regulation, passenger name record.

1. Introduction

In its communication on a strategy for a secure Information Society, the European Commission invited the private sector, in particular, to '*stimulate the deployment of security-enhancing products, processes, and services to prevent and fight ID theft and other privacy-intrusive attacks*'[1]. Furthermore, in the Commission's roadmap for a pan- European electronic Identity Management (eIDM) Framework by 2010, one of the key principles governing electronic identity management is that '*the system must be*

[1] Communication from the Commission to the European Parliament and the Council on promoting data protection by privacy-enhancing technologies [COM (2007) 228 final - Not published in the Official Journal].

Corresponding author: *Andrea Chiappetta*
E-mail: a.chiappetta@miuniversity.edu

secure, implement the necessary safeguards to protect the user's privacy, and allow its users to be aligned with local interest and sensitivities'.

Article 8 (*Protection of personal data)* of the Charter of Fundamental Rights of the European Union[2], Title II – freedoms, provides guidelines relating to the protection of personal data, including:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

The implementation of the General Data Protection Regulation[3] (GDPR), fully adopted last 25/5/2018, introduce heavy penalties for non-compliant organizations[4]. Since cyberspace is borderless by nature and open to everybody, any sensitive personal info passing through should be preserved to ensure the protection of the user's identity and other personal records. Electronic records (e-records) may be related to the health status of a patient, the personal credit-card data and/or food/goods preferences of online shoppers, etc. In general, e-records are actually information provided by the end-users and collected and managed by the service providers during the online transaction process. The loss of control of such information by its owner/user represents a risk to the user privacy.

One important type of such e-record is Passenger Name Record (PNR), which is the travel record for passengers, used by mainly by airline and travel agency databases but daily adopted by all kind of transport modes. PNR information can include the passenger's full name, date of birth, home and work address, telephone number, e-mail address, passport details, credit card details or method of payment, the names and personal information of emergency contacts, as well as details of any special meal requirements or seating preferences or any other similar requests. Databases of PNR data are normally hosted centrally, within an international reservation system. The sharing of passenger data amongst multiple data controllers and processors creates privacy risks, on the basis that not all of these actors may apply adequate privacy preservation policies. Moreover, by collecting and correlating information like "special meal requirements" or "seating particularities" or even by "efficient" use (profiling) of the same individual's name, inferences may be made about such sensitive issues as the religion or health condition of the passengers. The risk to the privacy of PNR processing has recently been deliberated by the EU Court of Justice (CJEU)[5]. It also requested stricter adherence to the data protection right: PNR processing, as performed today, is an intrusive type of personal data processing, because PNR data may reveal considerable detail about an individual, such as their travel habits, relationships, and financial situation, which may also include sensitive information. On the other hand, however, the importance of passenger data (today, PNR) processing in the fight against terrorism is unquestionable and several article are available on it. Apparently, however, PNR processing is considered by the CJEU to be so risky for the protection of fundamental rights that careful scrutiny needs to be made to the relevant regulatory text.

In summary, while e-records, such as the PNR, are important data for the smooth operation of the service providers, they do not provide sufficient privacy to the end users. Different service operators may only require access to specific subsets of the e-record in order to offer their services. In addition, sensitive personal information contained in the e-record may be exploited by third parties for undesired purposes, such as identity theft, unsolicited marketing (spam), etc. A cancelled or completed trip does not erase the record since copies of the PNRs may be retained indefinitely by airlines, and travel agencies or for post-trip requirements or to meet local legal requirements. It is important to safeguard and protect such on-line info and therefore, more research needs to be done in terms of preserving and

[2] Charter of Fundamental Rights of the European Union, Title II

[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)

[4] The lower level of fine, up to €10 million or 2% of the company's global annual turnover, will be considered for infringements listed in Article 83(4) of the General Data Protection Regulation. The higher level of fine, up to €20 million or 4% of the company's global annual turnover, will be considered for infringements listed in Article 83(5) of the General Data Protection Regulation.

[5] CJEU's Opinion 1/15 was issued on 26 July 2017 and was in relation to the lawfulness of EU's PNR Agreement with Canada. Specifically, CJEU adjudicated that the processing of PNR data generally pursues a different objective from that which was intended when collected by air carriers, and thus requires a different legal basis."

protecting the privacy of the sensitive personal data contained in existing e-records, whilst preserving the efficiency of online operations and services.

The worldwide system used to coordinate travel bookings between airlines, travel agents, and/or Online Travel Agents (OTAs) has security and privacy flaws, according to a recent research[1]. Some of the technology used by Global Distribution Systems (GDS), dates back to the 1960s. There is lack of built-in security and privacy by design in existing systems and in many websites and online service portals which control its access, making it relatively easy for a cyber-attacker to harvest personal information from online bookings. Such information can then be used by the hackers, for example, to craft convincing phishing emails requiring from the passengers to reveal even more personal information or financial information (payments)[6]. There appears to be no logging functionality in GDS systems as to who has accessed data and why, and in general, access controls are almost non-existent, allowing anyone from any company involved in booking to see the entire passenger record.

1.2 Privacy flaws in PNR and privacy enhancing technologies

This paper proposes a possible approach to manage the privacy flaws by proposing a new type of a universally applicable e-record that replaces the PNR, in a transparent and audited way of who accesses and what information about a passenger. Service providers will be able to share only partial (anonymized) information derived from the e-record than the whole PNR, as is the current case.

So, firstly, unlike current PNRs, the proposed e-record will be a structure, where each information element has a separate fine-grained, attribute-based access confidentiality and/or authorization policy. This means that different parties (service providers) can have access only in certain parts of the PNR according to the privacy settings (limited disclosure). The creation of a new type of PNR causes the entry of a new transaction in the blockchain. Secondly, every time a third party accesses a part of the PNR, a new transaction is created and linked to the original transaction overcoming the problem of current PNR of not knowing who has accessed what data and why. A block of transactions corresponds to the history of bookings made by a client without, however, revealing the identity of the traveller (to other parties apart from the PNR originator), and without each transaction containing more data than the minimum necessary required for the service. For example, a car rental transaction may contain data about the driver's age and insurance certificate without revealing the driver's name or address.

1.3 State of art

State of the art in Privacy Enhancing Technologies (PET) by proposing the development and validation of a next-generation universally applicable e-record, which will assure the preservation and protection of users' personal information, while facilitating the receipt of e-services (financial, travel, educational, and others) by the user. This new type of user-oriented e-record, termed *Anonymous Privacy Preserving electronic Record* will use the latest advances in *limited d*[7]*isclosure technology*, which provides a way of protecting individuals' privacy by allowing them to share only enough personal information with service providers to complete an interaction or an online transaction, while not revealing the true identity of the user (unless it is necessary to do so for providing the service or for security reasons), and in general not revealing more information to the service provider than necessary. Effectively, this is a (pseudo) anonymous user record whose link to the actual entity will not be available nor computable by third parties. It effectuates, among others, the basic data protection principle of data minimization, disclosing only personal information each time that is proportionate to the purposes and needs of the respective processing. The real identity of the user can only be revealed under specific conditions such as at the request of law-enforcement authorities (LEAs).

Limited disclosure technology uses cryptographic techniques and allows users to retrieve data that is vetted by a provider, to transmit that data to a third party, and to have these third parties trust the authenticity and integrity of the data. The cryptography technologies employed will allow being accessed even in 'unsafe' locations (e.g., over untrusted networks and intermediaries). This will make it a more flexible tool as even untrusted third parties can access approved information from this e-record in order to provide services.

[6] Olga Mironenko. (2002). Air passenger lists in civil aviation

[7] https://www.cbp.gov/sites/default/files/documents/pnr_privacy_3.pdf

The proposed concept represents a win-win solution, i.e., for both the service providers by achieving compliance with the GDPR, as well as the end-users (data subjects), by advising them that their submitted personal info is safe online. In this way, the privacy of the individual will be protected in the online environment.

It is fundamental implements the GDPR principle that requires both an implicit duty of care from the e-service provider to respect data protection legal requirements, as well as an explicit duty of care in being compliant to GDPR regulations (principle of accountability). There is a plurality of systems and methods for facilitating contractual agreements in both digital and analog forms[8]. The adoption of a blockchain allows for the disintermediation and the trust less exchange, where two parties are able to make an exchange without the oversight or intermediation of a third party, which in turn, reduces or even eliminates counterparty risk. Likewise, users are in full control of their personal transactions and their information. Due to the decentralized nature of distributed blockchain networks and systems, there are no single points of failure; hence users can rely on process integrity and have the confidence that transactions will be conducted and executed directly in line with blockchain protocols, unimpeded by third parties. By eliminating third parties, blockchain principles also deliver expedient transactions with zero transaction fees. The transparency and immutability inherent in blockchain ledgers are such that all parties of the transaction have full visibility, and previously committed transactions form a permanent digital record that cannot be deleted or modified, yet allowing changes and updates through new derivative records that link to the historical chain of data.

The paradigm proposed is fundamentally different when compared to related technologies, such as e-wallets. An e-wallet securely contains financial information of the user that enables the user to engage in a financial transaction with a third party. This information is mediated and/or guaranteed by a trusted third party- i.e., the provider of the e-wallet service. This will serve as proof of the service provision (in non-repudiated ways) that can be used by both the service provider and the service recipient (user), in a manner that protects and preserves the user's privacy.

The adoption of blockchain technology, which allows the efficient creation of auditable and traceable records showing the trace of data copying and sharing operations and allowing users and trusted third parties to verify that user privacy requirements have been respected[9]. This system of distributed trust allows lower transaction costs and speeds because the involved parties do not need to create and maintain contracts explicitly and implement new IT to setup enforce and monitor such contracts digitally. Limited disclosure technology uses advanced cryptographic techniques, allowing users to retrieve data that is vetted by a provider, to transmit that data to a relying party, and have these relying parties trust the authenticity and integrity of the data. In addition, existing advanced state-of-the-art open-source license-free blockchain technologies will be used and enhanced to reduce the design and implementation costs.

This approach to upgrading and expanding the use of e-records (known as PNRs in the travel industry) by establishing a comprehensive Methodological Framework, for raising awareness about public's privacy exposure in cyberspace, supported by an innovative new type of a more secure e-record, without exposing any of their personal data when dealing with online transactions. E-records represent the next generation of user private data being entirely under the control of the user. The tool should be designed and developed using open-source license-free software and offering open APIs to encourage third parties' development of relevant applications. To be useful the tool e-record will be vendor agnostic and open and applicable to a wide spectrum of online services[10].

The main 2 aspects to be covered and guaranteed are privacy and digital identity. This goal can be done using the Existing open-source license-free cryptography technologies will be leveraged and employed to define a methodology able to enable its online transaction by anywhere, including 'unsafe' locations.

The trail of transactions (blocks in the blockchain) could be used to establish a monitoring capability for an e-service provider that wants to keep track of the progress, for example, of this (anonymous) passenger during a trip (e.g. whether the passenger has paid for a ticket, boarded the train/flight checked in the hotel, etc.).

[8] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

[9]Data protection and security in civil aviation https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/JUR5630_lecture_11_11.pdf

[10]http://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html

Privacy (encryption, anonymization-layer): Allows the user to state his/her privacy policies and to select what user attributes to expose based on the service requested through a *differential relevance factor* (i.e., acknowledging that different services require different aspect of the citizen's data and adjusting the nature of the data shared based on that subset required). These preferences create appropriate encryption keys and configure the user agent, which is the only authorized tool to access the user e-record. The e-record is then stored in encrypted form by the user agent in local and/or cloud storage

Service Delivery layer: represents the interaction between the user-agent and the service provider. Service providers use portions of the e-record (permitted by the user) to create internal data records such as Passenger Name Records (PNRs)

Blockchain layer: The blockchain and associated infrastructure enabling service providers to create secure transaction/record chains.

The innovative concept is towards a private electronic record (e-record) used for transactions between the online user and the e-service provider, differentially adapting the nature of the data exchanged based on the unique semantics of the service provider, the data required to fulfil the service, and the specific subsets of that data relevant to optimising the privacy for the user. As such, the agent managing the user e-record is self-aware of the nature of the service being provided and, subsequently, providing the minimum information that needs to be provided on behalf of the user, and in support of the user.

The implementation of GDPR, by acknowledging that GDPR represents both an implicit duty of care from the e-service provider to respect privacy and data protection needs from the user, as well as an explicit duty of care in being compliant to GDPR regulations. This methodology also acknowledges the need for a digital contract between the service provider and the user, governing transactions between the e-service provider and the user, wherein the legislative consents are affirmed by the user, respected by the e-service provider, and an immutable audit point that either party can rely upon in the event of a dispute or disagreement. There is a plurality of systems and methods for facilitating contractual agreements in both digital and analog forms[11]. Due to the decentralized nature of distributed blockchain networks and systems, there are no single points of failure, hence users can rely on process and transactional integrity, as well as being confident that transactions will be conducted and executed directly in line with blockchain protocols, unimpeded by third parties. Due to the elimination of third parties, blockchain principles also deliver expedient transactions with zero transaction fees. The transparency and immutability inherent in blockchain ledgers are such that all parties to the transaction have full visibility, and previously committed transactions form a permanent digital record that cannot be deleted or modified, yet allowing for changes and updates through new derivative records that link to the historical chain of data. Further to the above, this instrument will allow selective negotiation of personal details and will help solve the problem of spam letters, e-mail, adverts, flooded inboxes, etc., as a result of exchanging details for online services[12].

1.3.1 The state of art in US and EU

Considering the state of the art, the implementation costs and the scope, nature as well as purposes of processing and the risk of changing probability and rigorousness for the freedoms and rights of natural persons, the processor and controller shall implement the right organizational and technical measure to make sure that there is an appropriate level of security to the risk, including of inter alia suitably:

a) Encryption and pseudonymization of personal data,
b) Being able to ensure continuous integrity, confidentiality, resilience and availability of the processing services and systems
c) Being able to restore the access and availability to persona data in an appropriate way in the event of technical or physical incident,
d) A process of continuous assessment, evaluation and testing the effectiveness of organizational and technical measures to ensure that there is security while processing[13].

[11] http://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html
[12] Voigt, Paul, and Axel von dem Bussche. "The EU General Data Protection Regulation (GDPR)."
[13] Security of processing. https://gdpr-info.eu/art-32-gdpr/

While assessing the right security level, there should be consideration on particular of the risks which are presented by processing, particularly from unlawful and accidental loss, destruction, alteration, unauthorized access to or disclosure of personal data transmitted, processed or even stored.

The processor and controller shall take the necessary steps in ensuring that any natural person operating under a processor or controller's authority with access to personal data has no need to process them, bar instructions from the controller, unless it is required to act like that by the State Law or Union member[14].

European Union data protection law set forth the following specific principles which have to be complied with for the processing to be legitimate.

Pertinence and necessity - The Controller should implement management practices to fulfil the obligation to collect only relevant and necessary data for a specified purpose.

Purpose limitation - Personal data is collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The Controller has a clear overview of all purposes for which personal data is processed. Personal data is not processed for purposes besides the original purposes, unless the (secondary) use is compatible.

Data minimization - Personal data collected by the Controller must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and further processed; if the same purposes can be realized in a less data intensive way a preference is given to that method.

Data update - Personal data is accurate, and, where necessary, kept up to date. Every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Data retention - Personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The Controller and/or Processing concerned should have processes and policies in place to:

a) determine what the applicable (minimum and maximum) retention periods are for the personal data that is being processed;
b) ensure that relevant retention periods are monitored.

1.3.1.1 User's e-record components

The user's digital identity (e-record) contains the profile and the credentials required to verify the user with service providers in a privacy-preserving manner. Credentials enable users to demonstrate attributes in an anonymous manner and to access services without disclosing their identity. By using limited disclosure credential technology, it also becomes possible to split identity-related information into a set of smaller statements that may be shown independently of each other. The new type of digital identity management system proposed in this proposal introduces pseudonymous credentials as a new element of the consumers' electronic record[15]. In this approach, the users' e-record comprises the following elements:

- *Authentication certificate*: The authentication certificate binds a public key to the identity of an individual. This is usually issued by a central authority, such as a Governmental Agency.
- *The signature certificate* is stored in the user' e-record. A single signature certificate is stored on the digital identity and any additional information pertaining to roles of the user is implemented by use of attribute certificates.
- *Attribute certificates:* Attribute certificates make it possible to model additional identity-related information about an individual. The X.509 standard[16] also addresses the format of attribute certificates.
- *Privacy Preferences Profile* (P3P profile): This allows the automatic negotiation between the user's e-record and the service providers websites about desired privacy settings.

[14] Voigt, P., & von dem Bussche, A. (2017). Scope of Application of the GDPR. In The EU General Data Protection Regulation (GDPR) (pp. 9-30). Springer, Cham.

[15] Functional Requirements for Electronic Records Management Systems. https://www.nationalarchives.gov.uk/documents/requirements.pdf

[16] The X.509 public key infrastructure (PKI) standard identifies the requirements for robust public key certificates.

- *Pseudonymous credentials:* Pseudonymous credentials allow a user to enjoy personalized services under a pseudonym and thus remaining anonymous towards the service provider. Only the root certificate authority can revoke pseudonyms and link them to the true user identity.
- *Digital documents/transaction records:* These are electronic records of transactions (bookings, payments) made by the users and are always at their disposal.

The above elements of the users' e-record could be stored in a Trusted Platform Module (TPM) or a designated secure element in their corresponding electronic devices, accessing to the TPM could be provided via an intuitive and user-friendly front-end User Interface, to monitor and to dynamically set their P3P profile policies[17].

The distributed nature of the ledger means that any collaboration between two parties under the ecosystem rules is publicly "announced" to all participants that maintain a copy of the blockchain. The blockchain servers of the participating parties preserve a time stamp on all transactions on the blockchain. They collect sets of transactions in blocks and publish a hash (a unique set of numbers that, if changed, shows the data or transaction is invalid) for each block of transactions with a time stamp to verify their authenticity[18]. Each owner of a transaction digitally signs a hash of the previous transaction and the public key of the other party and adds these to the end of the block. The validity of these transaction blocks is collaboratively performed by the blockchain participants through a process known as 'mining' which involves attempting to find a numerical value, known as a "nonce" which, when combined with all open transactions in a block, can be 'hashed' into a value that satisfies a certain "difficulty" but is also easily verifiable. Once the nonce is found by a 'miner,' the miner publishes the block with a hash to the rest of the ecosystem community.

1.3.2 Adoption of blockchain in transport modes

The transport industry has for a long time had great challenges and problems, affecting the way the stakeholders operate. However, with the invention of the blockchain technology, issues experienced in dispute resolution, tracking of orders as well as administrative challenges have been put under control. On a daily basis, there are about US $140 in funds held in disputes for the payments made in the industry of transportation[19]. On average, organizations are made to wait for about six weeks before they receive their payment. Administrative and processing costs have increased to as a high 20% of the overall costs in transportation because of relying too much on physical paper transactions[20].

The new platforms operating with blockchain will enable easy document coordination on a distributed shared ledger, eradicating the need for physical paperwork. With the use of smart contracts, customs clearance and approvals are made faster and in an efficient way, reducing the time spent in processing the goods shipped at the customs checkpoints. Companies need secure, updated as well as authentic data in decision-making. Blockchain in this regard makes sure that there is trustworthy data throughout the logistics and transportation system because the whole network contributes to the validation of data[21].

1.3.3 Anonymous credentials

Anonymous credentials means that the user never transmits the credential itself, but rather uses it to convince the verifier that his/her attributes satisfy certain properties – without leaking anything about the credential other than the shown properties. An advantage is that anonymous credentials allow the user to reveal a selected subset of his/her attributes, or even some property over the attributes, for example, that his/her age is over a certain number but not the exact age, or that her country is in a list of countries. In an online service transaction, multiple parties may be involved, and each of these parties needs different information from the user. For example, a travel service provider needs to know the traveler's current location but not his/her home address, while the bank that processes the payment needs to know his/her home address for verification. Also, for fraud prevention purposes, the travel

[17] https://www.ibm.com/blogs/insights-on-business/travel-and-transportation/tag/blockchain/

[18] Shmueli, Galit, and Travis Greene. "Analyzing the Impact of GDPR on Data Scientists Using the InfoQ Framework." (2018).

[19] https://www.winnesota.com/blockchain

[20] Voigt, Paul, and Axel von dem Bussche. The Eu General Data Protection Regulation (gdpr): A Practical Guide. Springer, 2017.

[21] Winnesota. How Blockchain Is Revolutionizing The World Of Transportation And Logistics [Infographic] https://www.winnesota.com/blockchain

service provider might want to ensure that the traveler has submitted his/her real identity to the bank, and not some bogus identity. The bank, in this case, plays the role of an identity escrow agent[22].

1.3.3.1 Anonymization techniques proposed

Examples of anonymization techniques include anonymization of records and logs, cookie removal software and trusted infomediaries that remove personally identifiable information. Various tools have also been proposed as "countermeasures to surveillance" to preserve online privacy in different scenarios, such as Bugnosis, remailers (e.g., Premail, mixmaster), Pretty Good Privacy (PGP), Dephormation, etc. Tree and graph-based techniques limited information disclosure requires the representation of personal information in fine-grained claims[23].

For efficient authentication of the claims from a user, a Merkle tree[24] can be suitably used in which all claims are placed at the leaf nodes of the tree[25]. This approach can ensure the integrity of the claims having the decision signed by a central authority, such as a governmental agency. This tree-based approach is implementable using an XML-based language and is scalable for authorizing multiple claims. Another approach for supporting limited information disclosure uses a user preference for disclosing specific information. Such techniques rely on appropriate preference relation models and graph-based representations.

1.3.3.2 GDPR and pseudoanonymization

GDPR clearly recommends that personal data be pseudonymized as one of the many ways of reducing risks from the direction of data subject, as a means used by data controllers in enhancing privacy. That will help in making it easier for the controllers in processing personal data beyond the purposes of collecting personal data or even processing of the collected personal data for any kind of use. The process of pseudonymization is used in reducing the possibility of personal data identifies and data records leading to a natural personal (owner of data) being identified[26].

With the GDPR, this is the first ever time that pseudonymization is being used in laws of protecting data as well as laws of privacy in the EU. Despite the fact that pseudonymization being recommended, it is not the ideal or easiest solution for all situations. Thus, while combining it with the right technologies is not an assurance out of the GDPR[27]. Pseudonymization enhances uncoupling of specific aspects of data from a subject of data, where the most sensitive and identifying pseudonyms replace fields of data in the record. The organizational measures and techniques include adhering to the privacy by principles of design (where pseudonymization is in GDPR) and methods like encryption, hashing and tokenization[28].

The GDPR introduces a new concept in European data protection law – "pseudo-anonymization" – i.e., rendering data neither anonymous nor directly identifying[29]. Pseudonymization is the separation of data from direct identifiers so that linkage to identity is not possible without additional information that is held separately. Pseudonymization, therefore, may significantly reduce the risks associated with data processing, while maintaining the data's utility. GDPR creates incentives for controllers to pseudonymize the data that they collect. Although pseudonymous data is not exempt from the Regulation altogether, the GDPR relaxes several requirements on controllers that use the technique.

The GDPR defines pseudo-anonymization as "*the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information10*." To pseudonymize, a data set, the "additional information" must be "kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person." In short,

[22] Nauwelaerts, W. (2017). GDPR-The Perfect Privacy Storm: You Can Run from the Regulator, but You Cannot Hide from the Consumer. Eur. Data Prot. L. Rev., 3, 251.

[23] https://www.i-scoop.eu/gdpr/pseudonymization/

[24] Merkle tree digital signature and trusted computing platform - Xiaofei, W., Fan, H., Xueming, T. et al. Wuhan Univ. J. Nat. Sci. (2006) 11: 1467. https://doi.org/10.1007/BF02831799

[25] In Proceedings of the 4th ACM workshop on Digital identity management - DIM '08. New York, New York, USA: ACM Press claims required by the service provider are revealed. https://dl.acm.org/

[26] Caruana, M.M., 2017. The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement. International Review of Law, Computers & Technology, pp.1-22.

[27] Personal data pseudonymization: GDPR pseudonymization what and how https://www.i-scoop.eu/gdpr/pseudonymization/

[28] I-scoop. (n.d). Personal data pseudonymization: GDPR pseudonymization what and how. Retrieved from https://www.i-scoop.eu/gdpr/pseudonymization/

[29] Voigt, Paul, and Axel von dem Bussche. The Eu General Data Protection Regulation (gdpr): A Practical Guide. Springer, 2017.

it is a privacy-enhancing technique where directly identifying data is held separately and securely from processed data to ensure non-attribution.

Pseudonymization is not on its own a sufficient technique to exempt data from the scope of the Regulation. GDPR also states that data which has undergone pseudo-anonymization, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person" (i.e., personal data). Thus, pseudo-anonymization is not intended to preclude any other measures of data protection.

The Regulation recognizes the ability of pseudo-anonymization to help protect the rights of individuals while also enabling data utility. Thus, GDPR allows controllers who pseudonymize personal data more leeway to process the data for a different purpose than the one for which they were collected.

Much research has been carried out about the extent to which pseudonymized data can be reidentified. This issue is of critical importance because it determines whether a processing operation will be subject to the provisions of the Regulation. The key distinction between pseudonymous data, which is regulated by the GDPR, and anonymous data, which is not, is whether the data can be reidentified with reasonable effort[30].

In conclusion, the GDPR introduces pseudo-anonymization into European data protection law, as a means of protecting the rights of individuals while also allowing controllers to benefit from the data's utility. Although pseudonymized data still falls within the scope of the Regulation, some provisions are relaxed to encourage controllers to use the technique. Thus, controllers that pseudonymize their data sets will find it easier to be allowed to exploit personal data for secondary purposes and for scientific and historical research, as well as to meet the Regulation's data security and data by design requirements. Where appropriate and where legally supported, the tool will utilize reversible pseudonym generation technologies where the user pseudonym can link to the true user identity when this is needed for financial and law purposes.

Conclusion

The issue of cybersecurity and privacy has always been a challenge in the transport industry. Companies and individuals are always concerned about their sensitive data being leaked or accessed by rogue individuals. With an increasing level of competition in the industry of transportation, organizations involved in the sector have to deploy the latest existing technologies and ensure extensive improvements on the quality of their services to stay in the industry. The key success factor in the transportation business is delivering the most efficient, flexible and cost-effective services. That is the major reason why ought to turn towards the latest trends and strategies in the industry of transportation to compete with the major players in the industry. Trends like safe with driver electronic devices, self-driving trucks, compliance and regulation, delivery of addresses, drone delivery, spreading airlines operating in low-costs and blockchain technology in the delivery of services have changed the landscape of transportation industry, as synthetically represented in this research paper. This paper aimed to tackled the issue of PNR Directive Adoption and the impact of GDPR and the different concerns held by customers when it comes to shipment and transportation providing suggestions and possible solutions to be tested in order to contribute and improve the security flows.

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at https://jsdtl.sciview.net

Funding

The authors received no direct funding for this research.

Citation information

Chiappetta, A., & Battaglia, A. (2018). The impact of privacy and cybersecurity on e-record: The PNR Directive Adoption and the impact of GDPR. *Journal of Sustainable Development of Transport and Logistics, 3*(3), 77-87. doi:10.14254/jsdtl.2018.3-3.6.

[30]How Blockchain is Revolutionizing the World of Transportation and Logistics https://www.winnesota.com/blockchain

References

Caruana, M. M. (2017). The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement. *International Review of Law, Computers & Technology*, 1-22.

Charter of Fundamental Rights of the European Union, Title II.

CJEU. (2017). CJEU's Opinion 1/15 was issued on 26 July 2017 and was in relation to the lawfulness of EU's PNR Agreement with Canada. Specifically, CJEU adjudicated that the processing of PNR data generally pursues a different objective from that which was intended when collected by air carriers, and thus requires a different legal basis."

Collin, T. (2018). *The difference between a Private Public Consortium Blockchain*. Retrieved from https://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html

Europa.eu. (2016). 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).

European Union. (2016). Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

GDPR Associates. (n.d). The lower level of fine, up to €10 million or 2% of the company's global annual turnover, will be considered for infringements listed in Article 83(4) of the General Data Protection Regulation. The higher level of fine, up to €20 million or 4% of the company's global annual turnover, will be considered for infringements listed in Article 83(5) of the General Data Protection Regulation.

IBM.com (n.d). *Insights on business travel and transportation*. Retrieved from https://www.ibm.com/blogs/insights-on-business/travel-and-transportation/tag/blockchain/

Intersoft consulting. (n.d). *Security of processing*. Retrieved from https://gdpr-info.eu/art-32-gdpr/

I-scoop. (n.d). *Personal data pseudonymization: GDPR pseudonymization what and how*. Retrieved from https://www.i-scoop.eu/gdpr/pseudonymization/

Lex.europa.eu. (n.d). Communication from the Commission to the European Parliament and the Council on promoting data protection by privacy-enhancing technologies [COM (2007) 228 final - Not published in the Official Journal] Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14555

Nauwelaerts, W. (2017). GDPR-The Perfect Privacy Storm: You Can Run from the Regulator, but You Cannot Hide from the Consumer. *Eur. Data Prot. L. Rev.*, *3*, 251.

Olga M. (2010). Data protection and security in civil aviation https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/JUR5630_lecture_11_11.pdf

Olga Mironenko. (2002). *Air Passenger Lists in Civil Aviation*.

Public Record Office. (1999). Functional requirements for electronic records management systems. Retrieved from: https://www.nationalarchives.gov.uk/documents/requirements.pdf

Shmueli, G., & Greene, T. (2018). Analyzing the Impact of GDPR on Data Scientists Using the InfoQ Framework.

U.S Department of Homeland Security. (2013). *U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy*. Retrieved from https://www.cbp.gov/sites/default/files/documents/pnr_privacy_3.pdf

Voigt, P., & von dem Bussche, A. (2017). Scope of Application of the GDPR. In *The EU General Data Protection Regulation (GDPR)* (pp. 9-30). Springer, Cham.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)* (Vol. 18). Springer.

Winnesota.com (n.d). How blockchain is revolutionizing the world of transportation and logistics. Retrieved from https://www.winnesota.com/blockchain

Xiaofei, W., Fan, H., Xueming, T., & Guohua, C. (2006). Merkle tree digital signature and trusted computing platform. *Wuhan University Journal of Natural Sciences*, *11*(6), 1467-1472. https://doi.org/10.1007/BF02831799

Journal of Sustainable Development of Transport and Logistics (ISSN: 2520-2979) is published by **Scientific Publishing House "CSR", Poland, EU** and **Scientific Publishing House "SciView", Poland, EU**
Publishing with JSDTL ensures:
• Immediate, universal access to your article on publication
• High visibility and discoverability via the JSDTL website
• Rapid publication
• Guaranteed legacy preservation of your article
• Discounts and waivers for authors in developing regions
Submit your manuscript to a JSDTL at http://jsdtl.sciview.net/ or submit.jsdtl@sciview.net