Distributed ledger technology and European Union General Data Protection Regulation compliance in a flexible working context

Domenico Rotondi | Marco Saltarella | Gaetano Giordano | Francesco Pellechia

Abstract
Compliance of distributed ledger technology (DLT) based solutions with the European Union General Data Protection Regulation (EU GDPR) is currently a hot topic both from a technical point of view, as well as from a legal and normative one. Flexible working is a new working model where employees can perform their work activity without specific time and space constraints. In this context privacy and information trustworthiness are relevant and, therefore, on the one hand it can gain benefit from using DLT based solutions, on the other hand it must comply with the GDPR. This paper describes a solution that combines DLTs and the new CipherText-Policy Attribute Based Encryption cryptographic techniques to support compliance with the EU GDPR in the context of flexible working. The devised solution is being concretely experimented, in the context of the EU H2020 CITADEL project, by the Municipality of Bari (Italy).

Keywords
blockchain, CP-ABE, DLT, encryption, GDPR, privacy, security

1 | INTRODUCTION

Flexible working is a new way of managing work activities where employees do not have strict time and place constraints in doing their work. Flexible working is not only envisaged as a way to improve work-life balance, and to enable more women to participate in the labor force, but also as a way to improve productivity and economic development. Indeed, this approach is also being pursued by Public Administrations (PAs) worldwide. In Italy, for instance, flexible working (Lavoro Agile in Italian normative) is explicitly envisaged by the law 81/2017, and specific measures for flexible working in PAs are provided by the law 124/2015. As an example Italian PAs must provide this form of working to at least 10% of their employees.

In these years there were many attempts, usually as pilot activities, to activate this new working approach and to concretely face old and new issues. Among them there are: how to support and document the right to disconnect and how to preserve confidentiality of employees' data while doing their work in flexible modality.

To this end properties like trustworthiness and authenticity are desirable, as well as the possibility to assure them without a trusted third party. Blockchain technologies can help on these aspects assuring trustworthiness, authenticity and immutability of exchanged data, though distributed ledger technology’s (DLT’s) transactions are accessible to all DLT's users. Data exchanged while doing flexible working are usually confidential, and some of them are personal data being able to provide hints on employee's life habits. Therefore, flexible working must also take into account privacy issues.

Currently the European Union (EU) holds the most advanced law, EU General Data Protection Regulation (GDPR), related to management of ethical issues in collecting and managing personal data. In EU, privacy and personal data protection are fundamental freedoms as stated in the EU Charter.

With the exclusion of some specific area (eg, public safety, law enforcement; see EU GDPR whereas clause 19), the EU GDPR has also unified, starting effectively from May 25, 2018, the privacy regulation for all EU citizens or people in the EU independently from their actual geographical location as well as from the service provider location.

EU GDPR covers and regulates, with the mentioned exceptions, all personal data collection and processing independently from the application domain. This is different from the approach and normative in other countries. Indeed, United States has not formulated an all-encompassing regulation, but sector specific data protection laws and regulations (eg, Health Insurance Portability and Accountability Act [HIPAA], Gramm-Leach-Bliley Act [GLBA], Federal Information Security Management Act [FISMA]) that apply together with state-level legislation. Canada has an approach that, to some extent, is similar to the EU one. Indeed, in Canada protection of personal data is regulated by two federal laws: Personal Information Protection and Electronic Documents Act (PIPEDA) for the private sector and the Privacy Act for the public sector. As for the United States there are provincial laws. The same can be stated for Australia whose privacy norms are stated in the Privacy Act 1988.

EU GDPR is, anyway, the regulation with the most extensive rights for users. It mandates managing the full life-cycle (from data acquisition, up to their destruction) of personal data. End-to-end data protection requires of course a proper combination of security features, usually encryption mechanisms. Additionally, many contexts are characterized by a relevant dynamic of subjects and it is often not possible to know in advance all subjects potentially authorized to access confidential information. As we transition towards the Web 3.0, and specifically to decentralized web, based on the so called DApps (Decentralized Applications), such strict privacy requirements may result conflicting with the decentralized approach. Blockchains as fully distributed and immutable ledgers of transactions offer: (a) decentralization (their distributed computational nature assures fault tolerance, absence of single points of failure, and attacks resistance), (b) trustworthiness (the main objectives of DLTs is to assure trustworthiness of exchanged data without the need of a trusted third party), (c) authenticity (each transaction is cryptographically signed and validated by each node), (d) immutability (blocks are linked together by means of cryptographic hashes and...
This paper proposes a solution that exploits CP-ABE, a novel encryption technique, in combination with advanced encryption standard (AES) to handle data on a permissionless DLT (e.g., Ethereum) in a GDPR compliant way, to support a pilot experimentation of flexible working by employees of the Bari Municipality (Italy).

In detail, CP-ABE is a novel asymmetric encryption scheme in which each user has its own private key which is associated with a set of attributes that are usually part of user's profile. When encrypting a message, the data owner provides an access policy that specifies which attributes and conditions must be owned and met to positively decrypt the message. Access policies are used to encrypt messages. Therefore, only users having their keys satisfying the policy will succeed in decrypting the data.

The paper is organized as follows: Section 2 outlines related activities, Section 3 provides details on our proposal, while Section 4 presents the use case in which our solution is adopted and Section 5 summarizes the main outcomes and future plans.

2 | RELATED WORK

Currently DLT technologies are being widely investigated. Agbo et al. have presented a survey on blockchain applications in healthcare, highlighting their pros and cons, and that further research is required to address all challenges especially regarding security and privacy. Similar studies are provided by the European Union Blockchain Observatory & Forum on DLT and GDPR compatibility, as well as DLT opportunities in government and public services. Rantos et al. have proposed a blockchain-based IoT framework to help processing personal data in a GDPR-compliant way. Kosba et al. have presented a privacy-preserving smart contract system that provides on-chain privacy and contractual security. Dorri et al. have proposed a blockchain-based architecture to enhance privacy and security in an automotive ecosystem. Muma et al. have provided useful guidelines for designing GDPR-compliant blockchain solutions.

This paper describes a GDPR's fully compliant solution focused on the flexible working context, addressing the challenges of personal data handling through disruptive technologies such as attribute based encryption and DLT.

3 | GDPR PRINCIPLES AND COMPLIANCE PROCEDURES

The devised solution uses the DLT as a mean to exchange data related to flexible working activities from the employee to the employer ICT systems, assuring trustworthiness, integrity, immutability and GDPR compliance (even if limited to the application context).

As requested by the GDPR, any system that processes personal data must follow the paradigms of privacy-by-default and privacy-by-design. Specifically, the privacy-by-design principle requires that the system envisions adequate measures to safeguard the confidentiality of personal and sensitive information since the design stage. The privacy-by-default principle, instead, requires that the default settings of the system guarantee an adequate level of protection of personal/sensitive data, and, at the same time, that there is a minimal level of data protection that cannot be reduced.

As highlighted in Section 1, given the immutability property of DLT, it is not possible to immediately and directly comply with rights stated in Art. 16 and 17 of the GDPR (right to rectification and right to erasure respectively). This suggests to not store data directly on the DLT but, instead, keep only the hash code of such data as a reference in transactions, and store the encrypted data off-chain. In this way, it can take advantage of the property of data trustworthiness provided by the DLT, as it can still verify data integrity and origin thanks to the hash value stored on the DLT. This also contributes to keep transaction costs low, as transaction's fees are directly proportional to the amount of data.

GDPR Art. 5 mandates that the data controller/processor must have legitimate reasons for collecting the data and be transparent about which data are collected and for what purpose and ensure that: (1) there are no illicit uses (Lawfully, fairly and in a transparent manner), (2) data are collected for specific, explicit and legitimate purposes (Purpose limitation), (3) are limited to those strictly necessary for the use case (Data reduction), (4) are accurate and up to date (Precision), (5) retained for no longer than it is necessary (Limitation on archiving) and, finally, (6) “processed in a manner that ensures appropriate security” (Integrity and confidentiality).

Specific cryptographic techniques should be used to guarantee protection and integrity of data and that their access is restricted to subjects explicitly authorized (e.g., database administrators should not be able to access plain-text users' data).

As evident, very few of GDPR requirements are automatically met by DLT technologies. Therefore, specific privacy measures must be deployed in order to satisfy these mandates.

In addition to deploying specific security measures, the flexible working context can leverage on the existence of a contractual relationship between the worker and his/her employer. Indeed, the employment relationship implies the existence of legitimate reasons to collect employee's data and of well defined procedures to manage those data (e.g., wrong office entrance/exit badge stamping rectification) that can help in assuring compliance with the GDPR when using a DLT in this context. In our flexible working system, GDPR rights have been fulfilled as described below:

- **Right of access by the data subject (Art. 15):** flexible workers are explicitly informed about what information is acquired, how it is collected, stored and processed.
- **Right to rectification (Art. 16):** a flexible worker must always validate acquired data and explicitly authorize their transmission. In case a worker erroneously transmits incorrect data, he/she can ask to rectify or erase them and, if necessary, submit a new transaction with the updated data hash.
- **Right to erasure (Art. 17):** any, even potentially, personal data stored off-chain is encrypted twice. A first AES encryption is applied using an ephemeral key generated on the worker's device. This AES key is then encrypted using a specific CP-ABE policy. By destroying the encrypted AES key, the personal data cannot be accessed anymore.
- **Right to restriction of processing (Art. 18):** the processing is limited to simply fulfill flexible working needs.
- **Right to data portability (Art. 20):** data collected in relation to the employee's flexible working activities could be hardly useful in other contexts. Anyway a flexible worker can acquire them according to the usual administrative procedures.
- **Right to object (Art. 21):** our solution does not envisage specific processing on the DLT, including profiling, that is not strictly related to support the flexible working.
- **Automated individual decision-making, including profiling (Art. 22):** as stated it does not perform DLT based processing covered by this article.
VALIDATION USE CASE

Our use case supports the Municipality of Bari flexible working pilot and its main objective is to certify the timing and location of flexible working activities, being these elements critical to assure compliance with contractual and insurance constraints, including assurance of the right to disconnect. Specifically, our system gives to flexible workers the possibility to virtually timestamp their “office entrance/exit.” The flexible working program devised by the Bari Municipality, indeed, gives the opportunity to any requesting employee to perform its office activities in flexible working mode for 1 or 2 days/week, starting from 6:00 to 22:00, with an arbitrary number of breaks, with the only constraints to guarantee a preagreed 2 hours Availability Period, and to total the number of working hours envisaged by their contract.

The system has been designed following the privacy-by-design and privacy-by-default paradigms. Therefore, on one hand collected and managed data are minimized, on the other hand information is never transferred or stored in clear. Indeed, the data to be managed in a trustworthy way can be summarized as: activity/break start/end time, employee ID and its location when he/she generates a start/end event. An Android App has been developed to support picking up this information on employee request and generate a suitable DLT transaction using the mentioned encryption techniques to transfer these data to the Administration ICT systems.

Ethereum is the DLT technology adopted as it supports a Turing-complete language to develop DApps and smart contracts. Being a permissionless DLT all transactions are public, and therefore the identified encryption measures are critical to assure confidentiality and GDPR compliance. Figure 1 depicts the system architecture for the Bari’s pilot.
The Lightweight Directory Access Protocol (LDAP) Directory Service manages user profiles in compliance with the DIT X.500 standard, the AuthN Service manages users' authentication in Proof-of-Knowledge mode, the Supervisor Application Service supports supervisors in producing reports about flexible workers activities they are responsible for, the Attendance Registry Service is the Municipality's service that manages the attendance registry, and the CIPEL Service is the Bari Municipality's ICT systems employees involved in the pilot use for their daily work.

In Figure 1 there are four additional components: the Flexible Worker App which is installed on the worker's Android device and used to acquire and transmit via DLT's transactions the worker's data, the Supervisor Web Application used by supervisors to analyze employees' activities and flexible working impacts on the PA performances, the Attendance Registry DLT Oracle that interfaces the Ethereum DLT with the Attendance Registry Service of the Municipality, and the AuthN DLT Oracle that interfaces the DLT with the AuthN Service.

Each flexible worker in the Enrollment Phase provides his/her employee ID, assigned by the Municipality, and freely chose a password, that is used only locally to derive a symmetric key to encrypt data stored on the worker's device. The Android app then generates a public/private key pair using Elliptic Curve Digital Signature Algorithm (ECDSA) and the secp256k1 curve, as well as the worker's Ethereum address, derived from his/her ECDSA public key.

Supervisors, instead, use their employee ID, assigned by the Municipality, freely chose their password, and, have their public/private key pair, generated with the same aforementioned modality, for the web application login.

Finally DLT Oracles have their ECDSA public/private key pair, used to secure communication on the DLT, and their Ethereum address, derived from the ECDSA public key.

Figure 2 depicts the overall data flow highlighting the data and infrastructures (ie, DLT and off-chain storage) involved with the user's activities. Since workers' geolocation data is subject to specific restrictions by the Italian law, the Android app encrypts this information with a specific CP-ABE access policy, so that this data in clear can be accessed only by specifically authorized subjects.

Each event transmitted by the Android app is actually sent via the DLT only after the worker has explicitly provided his/her consent (Figure 3).
5  |  CONCLUSION

The previous sections have described our solution that makes use of the Ethereum DLT to exchange and “certify” flexible working related information. Thanks to the CP-ABE encryption technique it is possible to protect confidential and personal information and assure GDPR compliance granting access to these data only to the subjects that meet the CP-ABE access policies. Our system stores hash values of the information on the DLT, while real data are encrypted and stored off-chain. To enhance compliance with the GDPR, information that could be subject to rectification or erasure is doubly encrypted: the actual data with an AES ephemeral key, and the ephemeral key with CP-ABE.***

The Bari Municipality pilot will run from Spring 2019 till end of September 2019 (end of the H2020 CITADEL project). The system will be assessed and refined during the pilot execution. It is planned to extend the system functionalities and to apply it to wider Flexible Working contexts in the near future.

ACKNOWLEDGMENT

This work has been partially funded by the European H2020 Project CITADEL under GA 726755.

NOTES

* Legge 22 maggio 2017 n. 81, “Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato,” GU Serie Generale n.135, 2017.
† Legge 7 agosto 2015 n. 124, “Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche,” GU Serie Generale n.187, 2015.
‡ See https://digitalfreedomfund.org/the-right-to-disconnect-to-what-extent-will-we-need-a-right-to-unplug-from-our-digital-lives/ and Art. 19 of Italian law 81/2017.
§ Art. 89 does not consider this principle incompatible with data collection for archiving, research or statistical purposes.
¶ Data for statistical analysis and research must be provided in aggregate form.
∥ This information is not only part of the signed agreement between the employee and the administration but also always available via suitable URLs in the system applications.
** Erroneous data can be managed using for instance measures described in the previous bullets.
†† The Italian law on flexible working (Art. 14 of Law 124/2015) explicitly forbids penalties for the purposes of recognition of professionalism and career progression of employees dealing their activity as flexible working.
‡‡ That is, when starting for the first time the Android app on its device.
¶¶ The password is not stored in any form in the system and is used to unlock supervisor's configuration data.
*** CP-ABE decryption keys are only needed by system’s DLT’s oracles and subjects authorized to decrypt workers' location. The worker's Android app only uses the CP-ABE Public Key and CP-ABE access policies. The possibility of compromising the system is therefore minimized and, in case, easily discovered and recovered.

ORCID

Domenico Rotondi  
https://orcid.org/0000-0002-5298-4449

REFERENCES

1. European Parliament Resolution. Creating labour market conditions favourable for work-life balance. Off J Eur Union. (2018/C 204/09). 2018.
2. World Bank. World Development Report 2019: The Changing Nature of Work. Washington, DC: World Bank; 2018:61:76–92.
3. Byhovskaya A. Overview of the National Strategies on Work 4.0: A Coherent Analysis of the Role of the Social Partners. Brussels: European Economic and Social Committee; 2005.
4. Weber T. Janus and the trade union challenge of digital technology. Transfer Eur Rev Labour Res. 2017;23(2):225-227.
5. Donini A, Forlivesi M, Rota A, Tullini P. Towards collective protections for crowdworkers: Italy, Spain and France in the EU context. Transfer Eur Rev Labour Res. 2017;23(2):207-223.
6. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07); Berkeley, CA: 2007:321-334. https://doi.org/10.1109/SP.2007.11.
7. Agbo Cornelius C, Mahmoud Qusay H, Mikael EJ. Blockchain technology in healthcare: a systematic review. Healthcare. 2019;7(2):56. https://doi.org/10.3390/healthcare7020056.
8. Lyons T, Courcelas L, Timsit K. Blockchain and the GDPR (Thematic Report). Brussels: EU Blockchain Observatory & Forum; 2018.
9. Lyons T, Courcelas L, Timsit K. Blockchain for Government and Public Services (Thematic Report). Brussels: EU Blockchain Observatory & Forum; 2018.
10. Rantos K, Drosatos G, Demertzis K, Ilionidis C, Papanikolaou A. Blockchain-based consents management for personal data processing in the IoT ecosystem. Proceedings of the 15th International Joint Conference on e-Business and Telecommunications—SECRIPT, July 26–28, 2018, Porto, Portugal. Vol 2. 2018:572-577.
11. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP); San Jose, CA. 2016:839-858. https://doi.org/10.1109/SP.2016.55.
12. Dorri A, Steger M, Kanhere SS, Jurdak R. Blockchain: a distributed solution to automotive security and privacy. IEEE Commun Magaz. 2017;55(12):119-125.
13. Muma S, Kappos D, Sumroy R. The Right to be Forgotten Meets the Immutable A Practical Guide to GDPR-Compliant Blockchain Solutions. The Center for Global Enterprise; 2019. https://www.dscinstitute.org/assets/documents/GDPR_Blockchain_Short_Final.pdf. Accessed July 10, 2019.
14. Cavoukian A, Chanliau M. *Privacy and Security by Design: A Convergence of Paradigms*. Ontario: Information and Privacy Commissioner; 2013.

15. Ross R, McEvilley M, Oren J. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (NIST Special Publication 800-160). Gaithersburg, MD: National Institute of Standards and Technology; 2018.

**How to cite this article:** Rotondi D, Saltarella M, Giordano G, Pellecchia F. Distributed ledger technology and European Union General Data Protection Regulation compliance in a flexible working context. *Internet Technology Letters*. 2019;2:e127. [https://doi.org/10.1002/itl2.127](https://doi.org/10.1002/itl2.127)