Darko Samardžić[1]

RECORDS OF PROCESSING ACTIVITIES (ART. 30 GDPR) IN ANALOGUE AND DIGITAL ECOSYSTEMS

Abstract

Records of processing activities or so-called procedure logs often are an important basis to understand data flows and risks. At a first glance art. 30 GDPR makes the impression that records of processing activities are created for documentary reasons to feed supervisory authorities. According to art. 30 IV GDPR records of processing activities have to be presented to authorities on request. Moreover, a procedure log is valuable for an organization to understand, manage and steer data effectively. It is risky not to have an overview about data used by different functions and people, in different entities and cultures, in particular for data exchanged cross over jurisdictions or with third parties. Additionally, the data world is becoming more complex, communication volumes, speed and latency are increased. The internet of things is penetrating all areas of organizations, society and states. Such developments do not only take place internally. Many interfaces connect internal organizational processes, applications or devices with external people, service provider, supplier, customer, consumer or authorities. Machine to machine communication is expanding. This is the digital sphere in parallel to the analogue world many people are still very much used to. To cope with this matrix of analogue and digital ecosystems and means the GDPR requires the use of different instruments such as risk assessments, data protection impact assessments, technical or organizational measures. One of the basics are the records of processing activities.

Key words: record of processing activities, personal data, processing, accountability, compliance, risk-/principle-based approach, risk assessment, data protection impact assessment, controller, processor, digital ecosystems, IoT (Internet of things), apps, algorithms

1. Accountability

Firstly, it is important to explain the idea, basics, scope, exceptions, content and the (digital) environment of Art. 30 GDPR.[2] Authorities can act rather strict,

[1] Vanredni profesor na Pravnom fakultetu Univerziteta u Zenici;
[2] K.-U. Plath, Verzeichnis von Verarbeitungstätigkeiten u K.-U. Plath (iz.) DSGVO/BDSG, Köln 2018, Art. 30 para. 1 i dalje.

imposing high fines, conducting searches or raising inquiries. It is necessary to holistically understand the legal impact in conjunction with technological and socio-economic developments. Internal organizational governance structure such as governance bodies, processes and cultures have to be seen jointly with external context. External already means in the spirit of globalization to understand different jurisdictions and culture. In digital ecosystem this is even more important because the cyber space is not bound to geographical boundaries. Digitization connects minds, devices and applications. An exchange of data is easily possible. In particular from a governance and compliance point of view it is important to assure an overview, to understand streams and content, risks and impact.[3] This is crucial for mitigating risk and avoiding liabilities. Furthermore, a good management of data may lead to advantages towards competitors or other players in analogue as well as digital ecosystems.

The accountability principle in art. 5 II GDPR requires the controller to be responsible for and be able to demonstrate compliance with art. 5 I GDPR.[4] Recital 82 emphasizes the collaboration needs with authorities: Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations. Hence, data protection regulations have to be interpreted in this spirit. Art. 30 GDPR enables a transparent overview on operations for further understanding, at least at a first glance.[5] The goal is not to document everything in detail. At the same time, art. 30 GDPR supports the principles stipulated in Art. 5 I and II GDPR by providing structured information which shall lead to comprehensibility.[6] Otherwise, it would be difficult for externals to get an understanding easily. Even data protection authority experts are not able to know all kind of organizations, process and data streams, all technologies, governance patterns and cultural developments. Records of processing activities function as an axe of the GDPR, enabling

[3] M. Braun, Compliance und Datenschutz u J. Wieland/R. Steinmeyer (iz.) Handbuch Compliance-Management, Berlin 2020, 1079ff.; M. Ferme/F. von Kummer, Datenschutzrisikomanagement u A. von Walter (iz.), Datenschutz im Betrieb, Freiburg 2018, 353 i dalje.

[4] S. Pötters, Grundsätze für die Verarbeitung personenbezogener Daten u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 5 para. 30 i dalje, 1 i dalje.; T. Herbst, Grundsätze für die Verarbeitung personenbezogener Daten u J. Kühling/B. Buchner (iz.), München 2018, Art. 5 para. 77 i dalje, 1 i dalje.

[5] N. Bertermann, Verzeichnis der Verarbeitungstätigkeiten u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 30 para. 2.

[6] Za praksu: M. Lachenmann, Organisationsstruktur Datenschutz, Rechenschaftspflicht u A. Koreng/M. Lachenmann (iz.), Formularhandbuch Datenschutzrecht, München 2018, 1 i dalje.

further data protection measures such as data protection impact assessment (art. 35 GDPR)[7].

If we look at the former regulations on data protection an active reporting obligation towards authorities was foreseen, irrespective of the real, contemporary need for review of such data. Controllers had constantly to report processing activities to authorities.[8] Moreover, these obligations were differently regulated in the EU member states.[9] Member states had the right to transform the directive on their own discretion. This is the idea of a directive respecting the different jurisdictions of the members. Here we can recognize the advantages and disadvantages of the differing EU legislations means, concretely the legal effects of Directives with discretion on transformation for member states and regulations with their direct effects in member states comparable to national laws.[10] Now recital 89 GDPR follows a more self-responsible approach. Recital 89 GDPR serves as an expression of transparency, effectivity and good administration.[11] Controllers have to maintain a procedure log on their own and show it on demand. An accompanying goal of the GDPR was to reduce bureaucracy. In addition, this understanding follows the risk-based approach. Supervision or even investigation can be required where incidents occur, requests are raised or doubts exist. But the simple storing of data does not lead to significant, structured compliance and improvements.

The principle of accountability is supported by many data protection building blocks in the GDPR. Art. 24, 32 can serve as examples.[12] Art. 24 I GDPR demands: Taking into account the nature, scope, context and purposes of

[7] S. Klein, Datenschutz-Folgeabschätzung u A. von Walter (iz.), Datenschutz im Betrieb, Freiburg 2018, 329 i dalje; N. Nolte/C. Werkmeister, Datenschutzfolgen-Abschätzung u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 35 para 1 i dalje; S. Jandt, Datenschutz-Folgenabschätzung u J. Kühling/B. Buchner (iz.), München 2018, Art. 35 para 1 i dalje.

[8] Art. 18f. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[9] Ch. Tinnefeld/H. Hanßen/Ch. Bausewein, Verzeichnis von Verarbeitungstätigkeiten u. T. Wybitul (iz.) Handbuch EU-Datenschutzgrundverordnung, Frankfurt 2017, Art. 30 para. 1.

[10] Z. Meskic/D. Samardzic, Pravo Evropske Unije I, Sarajevo 2012, 181ff.; W. Schröder, Art. 288 AEUV R. Streintz (iz.) EUV/AEUV, München 2018, Art. 288 para. 1 i dalje, 23 i dalje., 37 i dalje, 51 i dalje.

[11] N. Bertermann, Verzeichnis von Verarbeitungstätigkeiten u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 30 para 2.

[12] J. Hartung, Verantwortung des für die Verarbeitung Verantwortlichen u J. Kühling/B. Buchner (iz.), München 2018, Art. 24 para. 1 dalje; C. Piltz, Verantwortung des für die Verarbeitung Verantwortlichen u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 24 para. 1 i dalje; S. Jandt, Sicherheit der Verarbeitung u J. Kühling/B. Buchner (iz.), München 2018, Art. 32 para 1 i dalje; C. Piltz, Sicherheit der Verarbeitung u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 32 para. 1 i dalje.

processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Art. 34 GDPR is even more specific mentioning single measures such as pseudonymization, encryption, confidentiality, integrity, availability and resilience of processing systems and services. To be able to implement technical and organizational measures processing records are needed as a reference or to make it more vivid procedure logs serve as an axe of a vehicle. This may be rather easy for a few processes. It becomes more complex for global acting or multinational companies. It becomes even more complex in case of a matrix of analogue and digital ecosystems. Different IoT technologies and applications have to be understood, furthermore, the interfaces among each other and interfaces towards other systems or applications. Organizations have to admit that over the years and looking forward different systems are in use. Here data exchange and communication machine-to-machine has to be enabled.

Another example is art. 35 GDPR[13]: Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Data protection impact assessments have to be based on the data processing taking place within an organization or conducted by an organization. To mitigate risks in the best possible way updates of records of processing are needed. It is interesting that the first drafts of Art. 30 GDPR contained ideas of updates or maintenance, however, were abolished afterwards.[14] In the spirit of the principle of accountability (art. 5 II GDPR) in conjunction with the principles such as accuracy (art. 5 I GDPR) can be interpreted as need for maintenance and update.

To capture dimensions and players of data protection it is necessary to know core terms, to reflect GDPR risks and legal consequences. For the design of records of processing activities it is needed to identify personal data within streams, processes or applications. Art. 4 no 1 GDPR[15] defines personal data as: ‘means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name,

[13] A. von dem Bussche, Datenschutz-Folgenabschätzung u K.-U. Plath (iz.) DSGVO/BDSG, Köln 2018, Art. 35 para. 1 i dalje; N. Nolte/C. Werkmeister, Datenschutz-Folgenabschätzung u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 35 para. 1 i dalje.

[14] J. Hartung, Verzeichnis der Verarbeitungstätigkeiten u J. Kühling/B. Buchner (iz.), München 2018, Art. 30 para 31.

[15] P. Gola, Begriffsbestimmungen u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 4 para. 4 i dalje.

an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person‘. This already indicates the huge, complex matrix of data processed by an organization. In case of doubt or a firm link of different kind of data the nature of personal data cannot easily be ignored. Often the difficulty will even be the identification of personal data. An identification of data is aggravated through the broad definition of processing. Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (art. 4 no 2 GDPR)[16].

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (art. 4 no 7 GDPR).[17] Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (art. 4 no 8 GDPR).[18] These two definitions show that the controller is the primarily accountable person. There is no possibility to use company law for designing accountability. To determine the purposes and means of data processing leads to accountability. Nevertheless, art. 26 GDPR indicates that a joint controllership is possible.[19] This is in line with the content of art. 30 I a) GDPR taking into account the controller, the processor, representatives and the data protection officer.

As indicated in art. 30 I d) GDPR records of processing activities demand recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations. Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not (art. 4 no 9 GDPR)[20]. This shows that it is not enough only to identify data subject in the own organization. Data subjects at the other end of a data process have to be named as well. This leads to a more complete picture of participants. In a relationship

[16] T. Herbst, Begriffsbestimmungen u J. Kühling/B. Buchner (iz.), München 2018, Art. 4 Nr. 2 para. 1 i dalje.

[17] J. Hartung, Begriffsbestimmungen u J. Kühling/B. Buchner (iz.), München 2018, Art. 4 Nr. 9 para. 1 i dalje.

[18] P. Gola, Begriffsbestimmungen u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 4 para. 74 i dalje.

[19] C. Piltz, Gemeinsam Verantwortliche u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 26 para. 1 i dalje.

[20] P. Gola, Begriffsbestimmungen u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 4 para. 78 i dalje.

between two people this still seems easy but among many data subjects and in particular in digital ecosystems or huge communities this is more demanding.
Art. 30 II GDPR foresees obligations for the processor in parallel to the controller. These obligations are limited in contrast to the controller consisting of names and contact details, categories of processing, where applicable, transfer of personal data to a third country or an international organization and where possible, a general description of the technical and organisational security measures referred to art. 32 I GDPR. Due to the narrower knowledge base processors have fewer obligations than controllers. For instance, the processor can build categories of data processed. It just is a display of the own processing work. The exact purposes are or shall be known by the controller.[21]
In digital ecosystems identification obligations and workload can be rather challenging for processors. Digitization promotes more and more cloud service provider, hosting supplier or software as a platform busines models. This means that such service services are provided for many controllers. Here a proportionality and risk-based approach could lead be more reasonable. The processor could provide a list of all controllers serviced without going into deeper details. Authorities may request more details, decide whom to contact directly or to demand joint attempts.
Art. 30 GDPR entitles authorities to impose high fines. Art. 83 IV a) GDPR foresees that infringements of such provisions shall, in accordance with Art. 83 II GDPR, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year.[22] Legal proceedings are in the competencies of national courts. Interpretations of the GDPR belong to the Court of Justice of the European Union.

2. Scope

For sure art. 30 GDPR has to be applied to orgnizations with more than 250 employees. Crucial is the overall number of employees of a legal entity, not the number of employees participating in the processing of data in question.[23] This theoretically means a privilege for micro, small and medium sized companies. Risks in micro companies may be smaller and their capabilities for set up and maintenance of a procedure log limited. Overall, data protection rights are part of the fundamental rights and freedoms. This means in the spirit of practical

[21] J. Hartung, Verzeichnis der Verarbeitungstätigkeiten u J. Kühling/B. Buchner (iz.), München 2018, Art. 30 para 28.
[22] Th. Becker, Allgemeine Bedingungen für die Verhängung von Geldbußen u K.-U. Plath (iz.) DSGVO/BDSG, Köln 2018, Art. 83 para. 1 i dalje; M. Bergt, Allgemeine Bedingungen für die Verhängung von Geldbußen u J. Kühling/B. Buchner (iz.), München 2018, Art. 83 para 1 i dalje, 89.
[23] J. Hartung, Verzeichnis von Verarbeitungstätigkeiten u J. Kühling/B. Buchner (iz.), München 2018, Art. 30 para 35.

concordance that right and freedoms have to be balanced, at least respected as much as possible.[24] This is expressed in recital 13: 'In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.'

Art. 30 V GDPR foresees further application fields and exceptions: The obligations referred to in art. 30 I, II GDPR shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in art. 9 I GDPR or personal data relating to criminal convictions and offences referred to in art. 10 GDPR. Art. 9 and 10 GDPR regulate rather sensitive data.[25] Art. 9 captures processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Besides, the 250 employee-threshold is insignificant if the processing of data is likely to cause risks to the rights and freedoms of data subjects. These are rather indefinite terms and in case of doubt can be interpreted rather broadly. Additionally, each processing of personal data bears risks.[26] The original idea to exempt micro, small and medium sized organizations from data protection administration burdens is a bit naïve in the course of digitization. Even micro or small companies will increasingly be

[24] Z. Meskić/D. Samardzić, Pravo Evropske Unije I, Sarajevo 2012, 72f.; D. Samardzic/Z. Meskic, Pravo Evropske Unije II, Zenica 2017, 133 i dalje.

[25] T. Weichert, Verarbeitung besonderer Kategorien personenbezogener Daten, Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten u J. Kühling/B. Buchner (iz.), München 2018, Art. 9 para. 1 i dalje, 10 para. 1 i dalje.

[26] N. Lepperhoff, Dokumentationspflichten in der DS-GVO u RDV 2016, 197-203, 202.

dependant or use digital technologies. Finally, it seems that art. 30 V GDPR has not a broad field of application.[27]
Overall, the burden of proof is with the controller and processor.[28] They have to proof that there objectively is no risk for personal data. In digital ecosystems with growing data volumes, speed and latency of data exchange risks are increasing and data streams are not always transparent or the support of other participants is needed. Current cyber-attacks have shown that systems can be heavily attacked by hackers. In such cases it would be tough to estimate which level of internal cyber and data security is needed, to be able to reduce the likelihood of risks to rights and freedoms of others seriously.

3. Content

a. Responsibility of the Controller (Art. 30 I GDPR)

Art. 30 I a)-g) GDPR provides a certain content to be captured by records of processing activities. Single processes have to be named and listed separately.[29] Otherwise, a too condensed summary or a complex bunch of processes is not very supportive to understand data processing and review the lawfulness. Overall, most of the content required in art. 30 I GDPR is already requested by other provisions, e.g. 5, 6, 32 or 44ff.[30] Besides, the an overview about data processing and understanding should be in the own interest of a controller to get an adequate understanding, to enable insights, possibilities of fast response and preventive actions. Risks should be mitigated and liabilities avoided. Art. 30 I GDPR pursues the interests of data subjects, authorities, controllers and processors. If mistakes happen or breaches occur interests of all aforementioned parties could be damaged or suits filed.
Art. 30 a) GDPR requires the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer. Crucial is not the formal registration address, but the place you can meet or reach the controller.[31] For a review by the supervisory authorities it is not sufficient to know the place of a post box only.

[27] J. Hartung, Verzeichnis vn Verarbeitungstätigkeiten u J. Kühling/B. Buchner (iz.), München 2018, Art. 30 para. 39; Th. Müthlein, Neugestaltung der Auftragsdatenverarbeitung in Deutschland u RDV 2016, 74-87, 81.
[28] N. Bertermann, Verzeichnis von Verarbeitungstätigkeiten u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 30 para 5.
[29] Za praksu: S. Kremer/S. Sander, Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO) u A. Koreng/M. Lachenmann (iz.), Formularhandbuch Datenschutzrecht, München 2018, 156 i dalje.
[30] N. Bertermann, Verzeichnis von Verarbeitungstätigkeiten u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 30 para 1.
[31] C. Klug, Verzeichnis der Verarbeitungstätigkeiten u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 30 para 4.

Representatives (art. 4 no. 17 GDPR)[32], processors (art. 4 no 8, 28 GDPR)[33] and data protection officers (art. 37ff. GDPR)[34] are explicitly defined in the GDPR. To name the data protection officer makes sense due to the functions assigned and the expert knowledge. Jointly with good knowledge of the governance and culture, the strategy, business models and the digital technologies applied in an organization a data protection officer can be an adequate supporter and compliance manager.

Art. 30 b) GDPR requires to capture the purposes of processing. A data subject should be aware of the purposes of processing in the point of time of giving its consent. Recital 39 explicitly says: in particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. This is consistent with the idea of art. 6 I a) GDPR.[35] The purpose is the main reference of processing data. It is the reference for judging the lawfulness of processing.[36] The lawfulness test mainly is based on the test of proportionality and the principle of proportionality is an expression of the principle of earmarking.[37] Closely linked to these principles are the principle of transparency and full awareness of processing. Recital 42 points out: for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. The consent linked to clear purposes is an expression of the right to data protection self-determination. The purposes of data processing have to be as specific as possible. Recital 39 points out the importance of limitations by saying: The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. In addition, recital 65 clearly refers to the purposes on the right on rectification and erasure: In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they

[32] A. Klabunde, Begriffsbestimmungen u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 4 para. 71 i dalje.

[33] P. Gola, Begriffsbestimmungen u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 4 para. 74 i dalje.

[34] H. Heberlein, Datenschutzbeauftragter u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 37 i dalje; A. von Walter, Der Datenschutzbeauftragte u A. von Walter (iz.), Datenschutz im Betrieb, Freiburg 2018, 33 i dalje; za praksu: S. Kremer/S. Sander, Der Datenschutzbeauftragte u A. Koreng/M. Lachenmann (iz.), Formularhandbuch Datenschutzrecht, München 2018, 69-135.

[35] B. Buchner/Th. Petri, Rechtmäßigkeit der Verarbeitung u J. Kühling/B. Buchner (iz.), München 2018, Art. 6 para. 1 i dalje; S. Schulz, Datenschutz-Folgenabschätzungen u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 35 para. 1 i dalje.

[36] K. Marschall, Datenschutz-Folgenabschätzung und Dokumentation u. A. Roßnagel (iz.) Europäische Datenschutz-Grundverordnung, Baden-Baden 2017, §3 para 168.

[37] S. Schulz/P. Gola, Rechtmäßigkeit der Verarbeitung u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 6 para 30.

are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with the GDPR.

Art. 30 c) GDPR requires a description of the categories of data subjects and of the categories of personal data. Factually, this means to build clusters on people and data. People cluster can refer to different groups such as suppliers, customers, employees, authorities, joint venture partners or consultants.[38] Data clusters are more difficult to be set up. Besides the set up the maintenance is a secondary challenge. Data are increasingly processed by new technologies. The use of different systems leads to incompatibilities or at least interface challenges. Information such as clusters provide a basis for further data protection means such as data protection impact assessment (art. 35 GDPR).[39]

Art. 30 d) GDPR requires the listing of categories of recipients to whom personal data have been or will be disclosed including recipients in third countries or international organisations. The daily or operational recipients may be obvious. Furthermore, authorities, international organisations or data subjects in third countries have to be included. Art. 4 no 9 GDPR[40] defines exemptions on authorities: However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients. Internal data subjects must not be necessarily named. It is enough to use functional descriptions as long as a clear identification is possible.

Art. 30 e) GDPR requires where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of art. 49 I GDPR, the documentation of suitable safeguards. Here again we can identify the basic function of procedure logs as axe of data processing requirements. Data protection levels in other jurisdictions may be weaker.[41] Transfer of personal data has to conform to art. 44ff. GDPR[42]. It has to be judged if a processing to third countries is covered

[38] Ch. Haman, Europäische Datenschutz-Grundverordnung – neue Organisationspflichten für Unternehmen u BB 2017, 1090-1097, 1093; N. Bertermann, Verzeichnis von Verarbeitungstätigkeiten u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 30 para 7.

[39] Za praksu: M. Nolde, Datenschutz-Folgenabschätzung und Konsultation (Art. 35f. DS-GVO) u A. Koreng/M. Lachenmann (iz.), Formularhandbuch Datenschutzrecht, München 2018, 164 i dalje.

[40] P. Gola, Begriffsbestimmungen u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 4 para. 78 I dalje.

[41] N. Bertermann, Verzeichnis von Verarbeitungstätigkeiten u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 30 para 8.

[42] Za praksu: S. Weiß, Datentransfers in Drittländer u A. Koreng/M. Lachenmann (iz.), Formularhandbuch Datenschutzrecht, München 2018, 764 i dalje; Th. Zerdick, Übermittlung

by an adequacy decision (art. 45 GDPR)[43], by appropriate safeguards (art. 46 GDPR)[44], by corporate binding rules (art. 47 GDPR)[45], by a judgment of a court or tribunal and any decision of an administrative authority (art. 48 GDPR)[46] or according to derogations for specific situation (art. 49 GDPR)[47].

Art. 30 f) GDPR requires where possible, the envisaged time limits for erasure of the different categories of data. Erasure of data is of increasing importance. The term 'where possible' opens the field of interpretation. It can be factually understood as possibility to do so or only as an obligation in the spirit of the principle of adequacy.[48] We do see that more and more fines are imposed on breaches of duties on erasure of personal data. The implementation of art. 17 GDPR was one of the bigger evolutions in data protection.[49] Recital 39 demands: 'In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.' Recital 65 on right of rectification and erasure even uses the more informal, but in the public better known title of a right to be forgotten: A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. Nevertheless, the concrete kind and intensity of erasure is differently interpreted. At least, time periods for erasure shall be defined. Here procedure logs serve as management tool for review and follow ups. Recital 39 clarifies: 'The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and

personenbezogener Daten an Drittländer oder an internationale Organisationen u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 44 para. 1 i dalje.

[43] C. Klug, Datenübermittlung auf Grundlage eines Angemessenheitsbeschlusses u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, Art. 45 para. 1 i dalje.

[44] Th. Zerdick, Datenübermittlung vorbehaltlich geeigneter Garantien u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 46 para. 1 i dalje.

[45] C. Klug, Verbindliche interne Datenschutzvorschriften u P. Gola (iz.) Datenschutz-Grundverordnung, München 2018, art. 47 para. 1 i dalje.

[46] Th. Zerdick, Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 48 para 1 i dalje.

[47] Th. Zerdick, Ausnahmen für bestimmte Fälle u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Ar. 49 para. 1 i dalje.

[48] J. Hartung, Verzeichnis der Verarbeitungstätigkeiten u J. Kühling/B. Buchner (iz.), München 2018, Art. 30 para 23.

[49] H.-G. Kamann/M. Braun, Recht auf Löschung ("Recht auf Vergessen Werden") u E. Ehmann/M. Selmayr (iz.) Datenschutz-Grundverordnung, München 2018, Art. 17 para. 1 i dalje; za praksu: A. Koreng, Recht auf Löschung und Mitteilung (Art. 17, 19 DS-GVO) u A. Koreng/M. Lachenmann (iz.), Formularhandbuch Datenschutzrecht, München 2018, 595 i dalje.

further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.'
Art. 30 g) GDPR requires where possible, a general description of the technical and organisational security measures referred to in art. 32 I GDPR. Here again the procedure log serves as enabler to review the lawfulness of data processing.[50] Hence, this requirement at the same time protects the controller from unlawful processing or at least the possibility to reflect own proceeding. Art. 32 I GDPR follows a risk-based approach taking different aspects into account such as the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Measures such as pseudonymization and encryption indicate the growing importance of digital ecosystems. More and more applications such as clouds, apps or automated systems (e.g. robots, drones) are used. The more important is a procedure log to understand which applications are used with which safeguards. Technical, organizational measures may be besides default settings some of the most effective data protection measures.

3.2. Responsibility of the Processor (Art. 30 II GDPR)

In contrast to previous understanding the processor has own obligations in parallel to the controller. Art. 30 II GDPR stipulates four minimum requirements for processors or its representative processing data on behalf of ac controller: a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; b) the categories of processing carried out on behalf of each controller; c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of art. 49 I GDPR, the documentation of suitable safeguards; d) where possible, a general description of the technical and organisational security measures referred to in art. 32 I GDPR. In total, the obligations of a processor or its representative are limited in contrast to a controller. Criteria such as purposes are information originally belonging to the sphere of the controller.[51] However, essential duties such as transfer of personal data to third countries as well as technical and organizational security measures have to be documented.

[50] M. Martini, Verzeichnis von Verarbeitungstätigkeiten u B. P. Paal/D. A. Pauly (iz.) Datenschutz-Grundverordnung, München 2017, Art. 30 para 19.
[51] H. Gossen/M. Schramm, Das Verarbeitungsverzeichnis der DSGVO u ZD 2017, 7-13, 9.

4. Data Flows in a Matrix of Analogue and Digital Ecosystems

Art. 30 I GDPR is to be interpreted in the spirit of the core elements of the GDPR, following a principle-based approach (art. 5 GDPR). Accountability is part of the principle-matrix (art. 5 II GDPR). All principles, rights and duties have to be balanced in the spirit of practical concordance or fair balance considering the principle of proportionality and the risk-based approach. Hence, a procedure log has not to cover all dates possible in detail. But on the other side, complex structures, fast developing or risky digital technologies have to be captured transparently and logically.

A good example is the so-called right to erasure (art. 17 GDPR). In the last century this may have been easier in a paper administration. In digital ecosystems the different applications based on differing systems and interfaces constitutes another risk. If most people are asked honestly, they do not have enough insights and understanding. Even if a current technology is understood, there is a next invention coming. Hence, recital 66 explains needs on the so-called right to be forgotten: 'To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.'

Further examples for digital ecosystems are smart homes, automated systems in health areas or automated driving cars. Smart home ecosystems will develop further. Many strategic players are already in preparation. We do see that the heating, cooling industry, electric appliance manufacturer, food industry, energy suppliers, logistic providers, security service provider, automotive, infrastructure industry, cyber, data and other service provider process data (e.g. collection through sensors, big data analytics, processing through algorithms), develop strategies and business models. Additionally, state institutions such as mobility services or energy suppliers are of interest in this concept. Heating or cooling companies would like to know which climate is desired and which factors will influence the climate and how the different machines within and outside a house will communicate in regard to this. It is interesting to know times of attendance to regulate the climate at home or prepare the home temperature before people arrive at home. It is interesting if cars could communicate with the garage or houses to know times of arrival and leave. The car itself can be preheated or fed with information about the schedule of the day. Electric appliance managers would like to be allowed to identify the needs in a fridge to automatically inform the food industry or supermarkets about

supply needs. Logistic providers would like to get automated request for transport and delivery of things or people. Ecological synergy effects could be achieved by sharing cars or busses. Depending on the development of technologies new applications will arise.
Therefore, different industries intend to collaborate on data. Such data exchange and kind of collaboration raises other legal question such as on anti-trust, competition or intellectual property. Data processing will grow and become more complex. In a complex environment the first step is to create transparency. Overview and identification of data impact are a pre-condition to exploit further value for the own organization. Procedure logs will be a key to enable a fair processing of data and avoid conflicts in referring legal areas.

5. Design of Procedure Logs for Implementation and Maintenance

Different approaches on the design of procedure logs for implementation and maintenance can be used. On the one side this depends on the organizational circumstances and legal requirements. Specific data protection obligations have to be met. But such decisions increasingly interlace with further governance or compliance fields such as cyber security, data security, data confidentiality, trade secrets, intellectual property or constitutional and supranational law.
Another question is if a procedure log shall be process or application based. Efforts in the last decades were taken to establish more processes for more efficient and effective operations. Standardization was used additionally. The next level in growing, more complex, global systems is to create integrated processes. Often a huge matrix of end-to-end processes is used as basis. At the latest with the digitization a simple, clear picture became an illusion. Digital ecosystems follow a disruptive, agile development. The cyber space is huge and does not follow a certain structure. Hence, the process-based approach is to rigid. In such a interlacing, constantly updated or disruptive environment processes cannot simply be connected by interfaces. Process landscapes may be useful for an industrialization phase, for the manufacturing of a product. But digital services or the processing of data are different. Digital ecosystems are not linked to governance pattern from analogue ecosystems. Physical products are different from digital services. More and more physical products will be created on a digital bases or technologies. Hence, the more logical approach is an application-based procedure log. Applications may be added or exchanged without the need to adapt a complete process landscape.
Other decisions refer to the selection of internal or external design of a procedure log. Internally responsible people are familiar with existing organizational structures, decision makers, processes and cultures. Besides, internal people may be more cost efficient or passionate. External people may have use better or new tools, have more knowledge, experience or better networks. Besides, there is a certain distance to internal habits or cultures. At

the same time, the aforementioned advantages may be disadvantages. Missing knowledge on internal attitudes or behaviour may lead to implementation difficulties or even unacceptance. Overall, external solutions may be costly. Costs for external solutions can vary significantly. External service provider can only provide consultancy, IT support or a complete data protection service tool. Connected herewith is the maintenance. Procedure logs have to be updated. An update is more challenging in case of new systems without appropriate interfaces. Here costly tool solutions could be beneficial. This again depends on the pre-condition how much manual work or internal expertise is needed. It is questionable to what extent tools can autonomously identify and adjust content. Artificial intelligence solutions have to overcome a few challenges. Legal assessment and judgment can be partially executed by algorithms. But algorithms have to be programmed. Further abilities are provided by self-learning algorithms. But such algorithms bear other risks such as black box in the way of decision finding, application and control. To find an adequate answer on the question of internal or external design of procedure logs, a proportionality test following a risk-based approach may lead to adequate results.

Besides, methodological questions have to be clarified for the design of procedure logs in the light of adequacy. The question is on which knowledge can a procedure log be based? Records of processing activities can be designed by queries or interviews with selected people, functions, regions or cultures. Herewith the character of a procedure log is determined as well, more focused on criteria such as hierarchies, de-centrality or individualism. The governance and compliance principles of an organization shall be the scale for such decisions. Instead of such interrogative approaches, tools can be used. Tools again provide benefits such as increase of scale effects, the degree of standardization, the response time or evaluations. Finally, the programming, the use and the kind of result assessment determine the guidance. Such guidance has to correspond with the governance and compliance principles of an organization.

6. Conclusions

Without exaggeration, records of processing activities can be deemed as an axe of data protection. Procedure logs are part of the overall compliance and data management system. At the same time, it is a basis for core aspects of data protection such as risk management, data protection impact assessments and data processing. At least an overview about personal data processed is needed. It would be negligent to use data without transparency, without an understanding of content and impact. The complexity of data flows is increased by the matrix of analogue and digital ecosystems. The more, controllers and processors should be aware of data processed under their responsibility. It is not

an advantage to act in the dark. Digitization requires the identification, assessment and management of data risks. More connected things, smart homes and cities will increase complexity, overview and understanding. This automatically provokes the strengthening of principles of art. 5 GDPR. Transparency has to be established, integrity, confidentiality and accountability to be assured. The need for data protection impact assessments and privacy impact assessments will increase. The use of risky applications or other data processing has to be assessed timely. The follow up often will need an assessment and if needed, an adjustment of technical and organizational measures. Overall, it will be required to foster governance on data protection on the basis of art. 5 GDPR following a principle-based approach. Hence, records of processing activities are not a simple documentation but a basic instrument to comply to data protection regulations.

EVIDENCIJE O AKTIVNOSTIMA OBRADE (ČLAN. 30 GDPR) U ANALOGNIM I DIGITALNIM EKOSISTEMIMA

Sažetak

Evidencija aktivnosti obrade (EAO) je pregled nad postupcima kojima se obrađuju lični podaci. EAO se zahtijeva u čl. 30 Uredbe o zaštiti ličnih podataka. Stvaranje ovakve evidencije služi raznim funkcijama. Zakonodavac u čl. 30 IV Uredbe o zaštiti ličnih podataka želi omogućiti kontrolu kroz državne vlasti. Ali je ovo samo jedna funkcija iz vida državnih vlasti. EAO sve vise služi organizacijama da zadrže pregled nad svojim podacima i načinu obrađivanja. Organizacije koje sve više rastu ili postaju kompleksnije žele da zadrže pregled i kontrolu nad svojim aplikacijama i načinom obrađivanja ličnih podataka. To jos više važi u doba digitalizacije. Konekcija sa drugim aplikacijama, brzina i veličina izmjene podataka je toliko intenzivna, da EAO služi stvaranju transparencije. Izmjena podataka na internetu, u IoT (Internet of Things) ili komunikaciji između mašina (M2M, *machine to machine communication*) se može opisati kao obrada podataka u digitalnim ekosistmima.

Ključne riječi: *evidencija aktivnosti obrade, lični podaci, obrada, pouzdanost,* compliance, metodološki pristup na bazi proračunavanja rizika, procjena učinka na zaštitu ličnih podataka, voditelj obrade, izvršitelj obrade, digitalni ekosistem, IoT (*Internet of things*)