Protection of Personal Data in Computerized Accounting Programs

Mehmet Ali Yüzbaşıoğlu

Gaziantep Üniversitesi Oğuzeli MYO, Gaziantep, Türkiye
macmesaj@gmail.com

Abstract

One of the most vital accounting activities that businesses and organizations engage in is the essential planning and meticulous control of personal data collection and distribution. This task is particularly important in today's rapidly evolving landscape, where the nature of data management is constantly changing. The swift growth of new and innovative computer technologies has significantly influenced and transformed this crucial area of accounting practice. Computerized accounting programs are comprised of advanced and sophisticated software that effectively automates the entire accounting cycle, which in turn enhances both efficiency and accuracy in various financial record-keeping and reporting processes. As these advanced technologies continue to develop at an astounding pace, they not only streamline operations but also ensure compliance with ever-evolving regulations and improve overall data security. This results in the safeguarding of sensitive information, making it an indispensable component of modern accounting systems. In this study, a detailed research was conducted on the protection of personal data in computerized accounting programs.

Keywords: computerized accounting, personal data protection, data security

Introduction

Effective planning and careful control of personal data collection and distribution are absolutely critical in today's rapidly evolving and increasingly complex landscape of data management. The continuous and swift growth of technology has significantly reshaped the entire accounting field in ways that were previously unimaginable or dreamt of only in futuristic scenarios. Computerized programs, alongside advanced and sophisticated software solutions, now fully automate the entire accounting cycle, thereby boosting both efficiency and accuracy in the essential financial record-keeping processes that businesses rely on. These cutting-edge technologies

effectively streamline a vast array of various operations, significantly enhance overall productivity, ensure strict compliance with the ever-changing regulatory standards, and greatly improve robust data security protocols. This enhanced security plays a crucial role in protecting sensitive information that exists within modern accounting systems, which are at the core of many organizations. In this complex and dynamic context, it becomes increasingly important for organizations to prioritize the establishment of robust data management practices. These practices should not only uphold crucial confidentiality and integrity standards but also actively foster trust among clients and stakeholders in a technology-driven environment that is constantly evolving. The need for such diligence cannot be overstated, as it is foundational to sustainable and ethical business practices in our current age.

Research Purpose:

Data security is paramount in an organization's ability to safeguard sensitive information and maintain data integrity in the accounting information systems. Trust in each of the three data security elements—confidentiality, integrity, and availability—of the trinity triangle of information security is critical to doing so without worry. This is significantly more applicable in a computerized environment, given the volume of transactions and related information processed. Transactions in many firms flow through procedures that bypass a detailed human review. This lack of oversight is accepted given the reliance on computer procedures to safeguard data and increase accuracy. When individuals do access data, depending on what they are doing, they often only have access to specific subsets of information tied to their particular job functions.

Unfortunately, as more data are converted to electronic form and stored on computer systems, this data is increasingly a prime target. Security breaches, such as unauthorized computer hacking, pose a serious risk. In even very large organizations, database security breaches are more common than one might think. Because data security is so important, secure accounting information systems are of utmost importance. Public exposures of these security failures can produce considerable losses of reputation. Reliance on other systems can cause add-on losses. The need for security measures is evident from the damage caused by cyber assailants, who often have motives other than data theft. Firewalls, encryption procedures, user identities and passwords, and disaster recovery processes are commonly used to protect accounting information systems. Data security can help prevent more vulnerable computer systems from collapse. Security always includes physical security, but

physical security is the subject of other publications and is not discussed here. Preliminary security protocols, such as physical safety, must be in place before a serious discussion of data security can take place.

Like any policy, strict data security can also be communication, but the majority of security measures and procedures should be nearly or entirely transparent to the user. For accounting systems, losing accounting data can be much more damaging to an organization than losing software. A proactive approach considers what can go wrong and then develops a plan. Organizations usually name a chief information security officer or committee that will be responsible for maintaining an accounting (or broader organizational) security protocol. Keeping accounting IT systems safe serves as a simple list of procedures and questions.

Methodology

Computerized accounting refers to the use of software, data, and the World Wide Web for input, processing, and reporting of an accounting transaction. Broadly, this encompasses enterprise resource planning systems and the use of pre-developed accounting systems. Computerized accounting has two major benefits: it eliminates the need for humans performing redundant tasks while concurrently reducing the errors associated with those tasks; and computerized accounting provides, particularly with the use of enterprise resource planning systems, real-time financial and non-financial reporting for an organization. In contrast to computerized accounting, manual accounting is much more extensive and time-consuming because it does not involve the use of any electronic devices or systems. In addition to automating accounting processes, a great benefit of computerized accounting is the ability for individuals inside and outside the organization to have access to the accounting data. The creation of databases allows the storage and access of data to be reliable and readily available. One other major development from a technological perspective in accounting has been the increase in collaboration and teamwork facilitated through technology. This is particularly enabled through cloud-based software. A substantial benefit of new accounting software is that it is able to generate financial statements and reports without relying on human intellect. This information is not only produced more quickly but also is less prone to human error than financial reports obtained for manual accounting and is thus more accurate. Several software accounting packages also incorporate analytics that allow data analysis as part of the decision-making, which makes the accounting system even more valuable in satisfying an organization’s needs.

Findings

As the information and technology evolve and as computerized information systems become widespread, the need to ensure the protection of personal data, and not only this data, becomes particularly important. Given the high degree of concentration of personal data in computerized accounting programs, it is advisable to consider these valuable and privacy-sensitive resources as objects of particular threats or at least as newly emerged from the developed electronic environment that collects, processes, and uses them. Therefore, under these conditions, the establishment, development, and operation of a modern computerized accounting system should be carried out so that information resources are effectively and reliably used, and the protection of basic principles for the protection of personal data is observed. The legislative framework determines the protection of personal data in computerized accounting programs, but also the prevailing accounting theory contributes to the establishment and development of a secure computerized accounting system.

Conclusions

The future themes of the investigation could encompass the following new topics: the legislative framework for the protection of personal data in forces integrating the regulations on digital libraries and open science data; the presentation of the methodological approaches to provide scientific libraries with the information systems designed to process and analyze scientific visibility indicators; the scientific information evaluation models targeting the safety of personal data in big scientific data management with advanced protection measures; the criteria for the generation and use of scientific digital objects that are adequate in terms of personal data protection; the operational policies for scientific libraries designed to manage and preserve datasets with personal information; the development of a national repository for the preservation and use of scientific digital objects with particular attention to ensuring data privacy; the promotion of a sharing and trusted management model of personal data in the research and knowledge creation area; the identification of opportunities and evolution of blockchain technology at the base of platforms for the management and sharing of scientific research data in compliance with the privacy of personal data. Such themes ensure that scientific libraries collect, use, circulate, manage, and preserve personal data, thus playing an important role in a global scenario in which transparency and privacy will help realize the right of citizens to safeguard their personal data.

1. Introduction

One of the most important accounting-related activities is the planning, coordination, and control of the collection, processing, and distribution of personal data. The extremely rapid growth of the computerized component of new computer technologies, with a particularly high annual step, is also very pronounced in the above field. The content of computerized accounting programs consists of accounting software responsible for automating the accounting cycle (Korhonen et al.2021). This software has two essential characteristics: parametric accounting and parametric terms. In terms of parameterization accounting, the specificity of the establishment, the peculiarities of its activity, the impurity of the previous form in the scheme of accounting, the form of aggregation of the obfuscating moire, and its hierarchical level, as well as the basic data configurability or the accounting documentation flow providing the data, or the methodology of the data used or accounting information requests must be taken into account. At the same time, the guidelines, procedures, and control measures must be observed when fully protecting the legality and existence of personal data or any person (Kaissis et al.2020).

The integration of all CAF into a unit of computer that is part of the administrative program of the company will affect not only the business model, the relationship between administrators and workers, and the evolution of work in the future, but it will also involve significant changes in the accounting profession. The discipline and the legal norms that accompany accounting from its genesis suffer continual updating when applied to the technological level (Hasan, 2021). At different stages of accounting, and traditionally both properly, the accounting of the manual and the accounting of the automated system is consecrated to the sphere of personal and collective property. As an interesting paradox, the accounting of the automated system coincides, finally, with the organization of the accounting system, especially with the information. Starting from the existence of the computer model of the company, we find the cohabitation of two models of accounting: the computerized and the manual simulative. Accounting is based on the creative manual accounting of the society (Tsiligiris & Bowyer, 2021).

2. Importance of Protecting Personal Data

Personal data protection has become one of the most important problems in the information society. The dynamic growth of computer networks and the opportunity to get information from all over the world in real time have led to a faster increase in the role of the issue. Personal data is one of the most valuable resources of the

information society, quite often a basis for earning real money. People who want to steal or make improper use of personal data can be real experts who constantly improve existing and develop new intrusion methods (Deguchi et al.2020). A great variety of legal acts of different countries restricting and demanding control or secrecy of personal data may unpleasantly surprise the unprepared user of modern computer programs. However, it is necessary to analyze the legislative base in more detail and view in detail the tricks of malefactors from the point of view of laws and see the possibilities for their protection in modern computerized accounting programs. Protecting personal data is a more delicate issue than protecting common data acquired or created during the activity of a company, practical activities of physical and legal persons. Although third parties cannot legally get the information (common or confidential), they have the right and legal possibilities to control physical and legal person activities and can demand to surrender a copy of the accounting or tax data (personal data cannot be transferred to other persons than the person to whom they relate). Protection of personal data from illegal actions includes several problems. Firstly, it is necessary to organize the way to control this data. The possibility of checking who has taken a look at this data is very important. Secondly, while creating integrated computer programs, one should remember that the data processing cycles with personal data should be endowed with the protection means authorized in the legal acts. Moreover, means ensuring the rights of physical and legal persons to the data as their owners must be created. It is useful to create computer means that ensure prioritized protectability of information during data operations. This gives a possibility to legally privilege the persons related to a respective authority and access this data (Solove, 2024).

3. Legal Framework for Data Protection

The legal framework for data protection has evolved over the past few years mainly due to advancements in computer science and medicine. This scientific and technological evolution has increased the need to regulate the use and processing of personal data in order to protect the privacy and other legitimate rights of its holders. The field of protection of individuals with regard to the processing of personal data is safeguarded by several laws at an international level, with particular emphasis on the International Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Bulgakova & Bulgakova, 2023).

Data protection legislation has been present in several jurisdictions around the world. In the European context, the document of Directive 95/46/EC of the European

Parliament and of the Council, Basic Principles for Data Protection, is the landmark for the protection of personal data processing activities. This legislative decree aims to ensure data flows, as well as individuals' fundamental rights of identity and personal data protection. It also establishes general principles to be observed by data processing entities and outlines the rights and obligations of the holders, controllers, and processors of personal data (Veit, 2022).

3.1. General Data Protection Regulation (GDPR)

The use of ICT without securing personal data protection is a potential abuse and threatens to damage the trust of users in state institutions, corporations, and the system as a whole. Therefore, it is of utmost importance for all economic entities, including private accounting institutions, to take certain measures in order to maintain the levels of personal data protection. This is also especially important for PEs, law offices, notaries, tourist agencies, pharmacies, etc. In fact, all entities are obliged to protect the privacy of personal data subjected to ICT processing. The new regulation defines according to determined criteria what personal data is, what the processor is, and in which way the processor is determined. It also provides that the internal market shall not restrict the free flow of personal data, as it is in the interest to implement a stable, secure, and protected international data flow system (Dokuchaev et al.2020)(Vavoula, 2020).

The regulation, which has been developed in recent years and enters into force on a specified date, relates to the protection of personal data for natural persons, meaning that it is focused on all persons as stated in the regulation. It is based on previous directives and harmonizes personal data protection and privacy rules across the European Union and the European Economic Area and restricts access to various other global internet companies that collect personal data. It also addresses the export of data and personal data outside these areas. The aim of the rules is to have a free transfer of personal data from the European Union to other countries and to guarantee the creation of a new trade of personal data in the future. It does not matter whether the data controller is located in the EU or whether these rules can also be applied to external data processing for EU citizens (Veale and Zuiderveen, 2021).

3.2. Other Relevant Legislation

But the sectoral legislation does not restrict the rules and principles contained in it to personal data solely processed under its regulation because these rules are still general principles, rules that serve as a cornerstone of personal data protection and

that have been taken over by the general framework in specific treatments. An example of this is data accuracy or information, which is present in the Consumer Protection Information Act or the Code of Securities and Values. For non-specialized personal data, the software must be checked and configured to proceed to anonymization or dissociation of personal data, respecting the necessary security measures, in order to produce statistical data, in addition to the legitimate interest of public authorities in the use of personal data by these, since the realization of the public interest is necessary to the exercise of public power itself, previously delimited, in view of the justified expectations of society (Rahman et al.2020).

4. Principles of Data Protection

The General Data Protection Regulations set out rules for your business, which the computerized accounting program and service provider must also comply with. The principles for processing personal data are as follows, and the data controller is responsible for complying with these principles: (Hasal et al.2021)

1. Scrupulousness and Legality: Personal data must be processed in a scrupulous, legal, and fair manner. It must be processed for specific, clearly defined, and legitimate purposes, and there must be a legal basis for the processing. For example, when processing an employee's personal data, it is legal and legitimate for a contract of employment to be prepared. You may also decide for any other reason that you will process personal data; for example, to abide by a legal obligation or for legitimate interests. In any event, the purpose for which it is processed should be mentioned in the company's privacy information and preferably also communicated directly. It should even be taken into account that special categories of personal data are not processed without an appropriate legal basis. Under no circumstances should personal data be further processed in a way that is incompatible with those purposes (Ali and Hussain, 2024).

2. Proportionality: Personal data should be processed to the extent necessary for specific purposes. It should not be processed unless it is necessary. The company should avoid keeping personal data that is not necessary and process it in a proportionate manner compared to the purposes being pursued. Any period of data retention must be the minimum necessary, and the company must establish for each category of personal data of the persons concerned the duration of the time in which the personal data is kept (Nguyen et al., 2022).

3. Integrity and Data Confidentiality: Personal data must be processed in such a way as to ensure an adequate level of security. In particular, personal data must be safeguarded against unauthorized processing or unauthorized access to that data and to the computer system on which the program is located. In particular, personal data should be protected through appropriate technical and organizational measures against accidental loss or alteration, and against unauthorized or unlawful destruction, or illegal disclosure of, or access to, personal data transmitted, stored, or otherwise processed. It is important that a balance is found between the security measures implemented and the risks presented by the processing and the nature of the personal data that requires protection (Bulgakova & Bulgakova, 2023)(Haque et al., 2022).

4.1. Lawfulness, Fairness, and Transparency

The principle of lawfulness requires that personal data be processed in accordance with the rules of the law and that data controllers comply with these rules. This principle allows individuals to know what happens to their personal data and the purposes of their processing. Transparency ensures compliance with the principle of lawfulness. The data controller must provide the data subject with specific information about the processing of personal data. In order to do so, the information about the processing must be communicated to the data subject in a clear and accessible way. Both of these principles are closely linked to the right of the data subject to information and transparency (Thapa & Camtepe, 2021).

Certain measures must be taken by the data controller in order to allow data subjects to effectively exercise their right to information and transparency. As a first step, the data subject has the right to access the personal data. The data controller must provide the data subject with concise, transparent, intelligible, and easily accessible information. The information must be provided without delay and at the latest within one month. This period may be extended by two months, especially when requests are complex or numerous. When the data subject submits the request by electronic form, the information must be provided by electronic means. In the event that the requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive nature, the controller may charge a reasonable fee or refuse to act on the request. In these cases, the data controller must provide the data subject with information on the measures taken. During the information phase, the data controller is not always obliged to provide the data subject with all the information (Kaminski2021)(Viljoen, 2021).

The data controller must provide confirmation to the data subject that the personal data concerning him are being processed and, if it is the case, access to the personal data and the following information: the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations; where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; the right to lodge a complaint with a supervisory authority; where the personal data are not collected from the data subject, any available information as to their source; the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. It is interesting to note that these obligations are very similar to the information obligations stated in the previous data protection legislation (Barati et al., 2020).

4.2. Purpose Limitation

Limitations of the purposes for which data may be used are referred to as subject-specific limitations. The data's processing must meet very specific pre-determined legitimate program-related purposes and be registered or documented. After personal data is processed for its purposes, this data may no longer be processed, unless another purpose is defined in another statement satisfying the other conditions. It is strictly forbidden to reprocess non-complying non-program-related data for a purpose other than the legitimate purposes defined in the operation. The limitation of the purpose is the most effective solution in avoiding the deviation of the processed data from the subject or purpose of the original data. While it may limit the data's usefulness, it considerably reduces the possibility that the character of data processed will evolve sufficiently far from the original character. The aim of this limitation is to inform the interested party as accurately as possible and the data subject where information about the recipients is particularly sensitive for the purposes to stipulate, prior to the processing. The data manager must, therefore, take into account the changing environment in making the purpose statement as much as possible. The situation in which the data is required and the data specified in the declaration should be well documented. In the practical reality of the declaration of objectives, this provision will have a positive effect. In addition, the provision would

directly lead to the establishment of 'legitimate' codes of conduct and the monitoring of the processing of personal data for purposes other than those defined in these codes of conduct endlessly (Müggenburg, 2021).

4.3. Data Minimization

Data minimization means that only personal data which is necessary for the business purpose should be collected and that the data should not be stored longer than it is necessary for the business purpose. The personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Data minimization is, in some sense, related to the principle of purpose limitation. However, while purpose limitation is related to the necessity to specify a valid purpose for data processing in the first instance, data minimization is concerned with whether additional personal data should be collected and with the question of what kind of personal data can be processed over the course of the business process. To a great extent, data minimization is linked to the quantity of the processed data. Ideally, when designing and implementing computerized accounting systems, organizations should establish a policy to minimize the data collected. This means that organizations should choose the least intrusive accounting software to handle the specific operations (Cavoukian, 2021).

4.4. Accuracy

In terms of its consequences for accounting, accuracy should be considered as the truth of every recorded piece of information. In other words, accuracy is essential in financial accounting. While the capture of the data affects the program's functionality in terms of utility, the data entered into this program at an inaccurate scale will also have serious consequences for the usability of the program and the information obtained from it. Because of entering the data inaccurately into computer accounting programs, there is no confidence in the recorded information. Usable information cannot be obtained if the input is not reliable. Of course, there are also value density problems; then the capture dimension comes into play while capturing the data into the system. For example, obtaining data from sales invoices that are not recorded in cash invoices, that is, recording the transaction as a sale will also cause a value density error (Ahrens & Ferry)(Hossain, 2024).

4.5. Storage Limitation

Principle 5: Storage Limitation. Personal data shall be 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. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to the implementation of the appropriate technical and organizational measures required to safeguard the rights and freedoms of data subjects. 1. Controllers must clearly define the retention period for personal data. This is linked to the purpose of processing the personal data. For instance, shoppers who purchase goods from an online clothing store may want to be able to see a record of what they have bought for at least five years after the purchase, as they may need proof to enforce their guarantee rights. Therefore, the online clothing store might want to be able to hold a record of to whom it has sold what for five years. Data collected via CCTV for security purposes may only be kept for a few days or weeks at the most, as the shop will be aware of any security issue within a short amount of time (Murdoch, 2021).

4.6. Integrity and Confidentiality

Integrity is the third of the pillars of security and confidentiality. Integrity encompasses the protection of the data contained in the accounting record from being modified by unauthorized persons or programs. In other words, without integrity, it is not possible to ensure that there has been an unauthorized modification of the data. Integrity refers to the maintenance of the correctness and security of the data. The objective of integrity is to prevent unauthorized persons from making changes to the information. Consequently, integrity is intended to protect against modifications to the accounting data by unauthorized persons. In general, computer security has been achieved if its three pillars are established: that is, what is selectively known is modified exclusively by those who have the right to do so, and that it is granted to those who have the right to consult it (Griffin et al.2021).

5. Security Measures in Computerized Accounting Programs

Security is an important factor in accounting software. Security measures outside the computer can be important. However, good computer software will allow the computer security itself to control access to computer resources. The computer should be within a secure environment, such as a locked room; access to the operating

system should be limited to responsible persons. Access to data files and programs should be by password identification of authorized users and run with user rights to protect the system from viruses. Transmission of data between the computer and, in some cases, remote terminals should be done over secured lines using encrypted messages. The computer and accounting software need to be secure. While computer security in a network is beyond the scope of this report, security awareness must be considered. Access to accounting modules from the outside should be through a secure virtual private network connection. From our real-life experiences, we can observe that most accounting systems are constructed using spreadsheets or database software, which is not recommended when handling confidential information. Manual recording and recording utilizing non-specialized software constitute a threat to sensitive employee information, primarily the accompanied risk of unauthorized access, unauthorized change of information, and distribution of falsified information. Unauthorized access can be removed with a systematic regulation that only certain personnel have access to the payroll and statutory reports. However, members with rights to access these records can, nevertheless, change any information and distribute falsely modified data without any application-level controls of these activities. To secure the system and solve these identified limitations, computerized accounting programs, including form programming, segregation of duties, automatic approval forms, network and password protection, and role permissions have been introduced. The programming requirements of the system are highlighted in the pattern of example computer record forms(Faccia & Petratos, 2021).

5.1. Access Controls

Access control is the control of who can and cannot access what information. It is related to the task of protecting information created and stored in a computerized accounting program from inappropriate access. Access control techniques help to ensure that only authorized users and systems are able to obtain access to accounting information. Accounting software must provide mechanisms to control and restrict access to classified and sensitive information, and ensure only authorized people have access to it. The primary way to control access is through user identification and authorization using passwords, as required by laws and accounting standards. No user should have access to more accounting data than necessary to perform their job. Accounting software should not have user accounts used for all activities. Users should log on to accounting software with individual user identification and have activities executed under that identification. If possible, the use of individual

passwords should be limited and, if necessary, dual responsibilities should be implemented. Multiple tax user identifications by the same person should be avoided for the purpose of workflow design and separation of duties. The period of time during which the user must enter the warehouse should be as short as possible. User identification and password selection in the hopes of reducing this time violate principles of independent choice, frequently changed passwords, rational password duration and complexity, secure private management, and banning the use of any shared accounts. Software should also meet the maintenance of user license and password history requirements (Faccia & Petratos, 2021).

5.2. Encryption and Decryption

The principal idea of encryption work is that plaintext is replaced by an equivalent ciphertext according to a previously agreed-upon procedure. Only a person who enjoys the knowledge of the method of encryption can convert the ciphertext back to the plaintext. In other words, this person has the confidence to revert the process of encryption. There are two approaches to the solution of the problem. The first possibility is to prevent unauthorized persons from gaining access to the given document through the use of a cipher that does not allow someone not knowing the method of encryption to conclude upon the plaintext or which does not give the plaintext even when extensive concrete examples of the same plaintext in a transformed form are given. The second approach is to protect the method of encryption from unwelcome spectators and unauthorized individuals. In carrying out the encryption, the precondition is that encryption with the given key may take an amount of time of not more than five times encryption with that same key. Special symbols and numbers have been defined for the formation of key sets. These are the input and output techniques which are carried out through the keyboard display for a direct connection with the user (Li et al., 2023)

The method of decryption is somewhat different from the one used for the transformation from plaintext into ciphertext. It would be most simple if the method of encryption itself could simply be used without having to inform the person who intended to convert the document from its transformed state. Practical assumptions disallow the everyday use of this method. If the method of encryption is only shared by the expected and the recipient, the method of decryption is insufficiently difficult for an unauthorized person to be able to completely decode the document with little effort. The only way of preventing this type of development is to select a cipher that is difficult or nearly impossible for unauthorized individuals to solve and which will

take these individuals a very long time to perform the computation. Any significant movement toward the solution of these ciphers will soon mark the beginning of a new scientific discipline named forward codification or forward encryption. The inserted level of forward encryption must be selected in such a manner that an unauthorized person cannot easily determine the plaintext of some interval of ciphertext. This person must convert the ciphertext with a less than 0.1% probability into the plaintext (Chowdhary et al.2020)(Ren et al., 2020).

5.3. Backup and Recovery Procedures

A lesser-known method of sabotage, though still possible on all types of programs in use, is the deletion by the authorized user of essential tables of the program. If there is no structured relationship between them, rebuilding those from backup files is very hard and involves the risk of losing current data through this process. One option could be restoring the principal tables into accounts lacking that type of transactions, and after that, manually reinstating the lost transactions in the table. The activities involving the risk of deleted transactions or tables are either those performed by the authorized user or the operation of programs recording the transactions. A task of the authorization system is to guarantee that these kinds of operations are performed by the same users who run those types of programs that generate these operations (Esposito et al., 2021).

First, because a user dedicated to backing up has no interest at all in deleting important tables. Moreover, if a user deletes the tables of another user, the latter cannot be stopped in their action, initiated with the program log-off request, and no message of delay from the system is sent to any of the monitoring means. A large extent of damages, foreseen to occur after a row or column-level deletion, may not happen, or the recovery funds may be achievable when the deletion of the tables has actually occurred (Brown & VanLehn, 2020).

6. Data Breach Response Plan

In the event of a personal information breach, the data protection officer shall submit a 24-hour personal information breach report, including the description and the details of the personal information breach. If the breach is confirmed after sending the 24-hour breach report, the data protection officer shall then submit a complete personal information breach report, including also the information and undertakings to the data subjects. Where, in connection with a personal information breach, the data protection officer reasonably expects that the rights and freedoms of natural

persons have been violated, the personal information breach report shall be immediately submitted, and the data protection officer shall inform the supervisory authority directly. Information shall be provided to the natural persons regarding the data breach that has occurred as soon as possible, unless prohibited by law. Such information can be determined as extensive if there is reasonable suspicion that the personal information breach may cause considerable harm to the rights and freedoms of natural persons (Daigle, 2021).

The supervisory authority shall also be informed about a personal information breach within three days after the receipt of the notification and not later than 72 hours after confirmation of the personal information breach, submitting a short description of the personal information breach, and shall perform the assessment of whether the data breach needs to be reported and published for the public by the supervisory authority. Said report can be delayed only as long as it is absolutely necessary, and the reasons for the delay of the report shall be explained in a mandatory manner. In case of publication of the report, the supervisory authority can also limit the scope of the agreed information. The data protection officer shall keep records of personal information breaches and give them to the supervisory authority upon request (Vojković et al.2020).

7. Auditing and Monitoring

Introduction Computerized accounting programs store and process an important amount of personal data. This data is included in different documents that, as a rule, represent a reflection of the main business operations. Some of the most important documents are sales and purchase invoices, payment and collection forms, payroll documents, as well as inventory movements. This means that an important amount of personal data can be found in the accounting data of every company. It is then important to protect this information against the rights of data subjects. Moreover, in relation to computerized accounting, we have to keep in mind that this information will finally be included in the annual accounts of companies, which will be available to the public (Turner et al., 2020).

In relation to compliance with the rights of the people that can be affected by the processing of this information, we can say that there is only one requested operation with respect to the personal data included in computerized accounting programs that has a specific development inside the GDPR, which is the provision of exercise of the rights of the data subjects. It is determined that “where processing of personal data is carried out by a small enterprise, an exception should apply to the obligation to

address a request described in paragraphs 1, 2, and 3 of this Article if that request is not manifestly unfounded or excessive, taking into account whether the processing is occasional and the nature of the data." This means that every information collector will have to have the capacity to respond to the right determination of data subjects (Zaeem and Barber2020).

8. Employee Training and Awareness

Because adequate security of personal data is not only demonstrated by technical measures, abilities, and good work practices, this policy also needs to take into account employees' awareness. Programs for professional training and awareness are of different character – from computer-based training to thematic folders, posters, websites, and local intranet. Thorough postulates and processes start when employees are educated. You must add to this policy consideration of the financial implications of possible mistakes in good protection failure. A person who is aware of possible mistakes or dangers in a situation must think before plunging in. Therefore, it costs you. Good and continuous personnel training is a part of a safety culture's computerized accounting program. The training's goal is to make personnel familiar with safety and to adapt staff to the level of security; they reflect not only their training in the security program (Zhang et al.2020)(Bisbey et al.2021).

Education must be repeated, and employees must change as their duties and software tools evolve. You can extend their awareness of potential security issues in daily or outside work routines. The program includes at least marking processes. An employee at the trainee's first recruitment must become thoroughly conversant with the procedures and the influential tactical protection policies. Each operation must be executed as required. All documentation must be typed. Afterward, the recruit must join another employee. In practice, during training, the tutor must observe all processes and the employee's adherence to marking procedures and train the formation of a protection culture. All observations must be marked by the manager and reported to the item's leader. After completing the qualification program, the final test must be passed. Results must be saved in the human resources department's personal file of the employee. In protective policies, the employee training improvement will occur throughout personnel provision for successful performance (ElMaraghy et al., 2021)(Marion and Fixson2021).

9. International Data Transfers

The Directive only more or less regulates the processing of data within the EU or the EEA. As a rule, personal data must be processed only in those places where adequate protection is guaranteed. Thus, the principle of not delivering data abroad is fundamental. The transfer of personal data to companies based in the USA is especially problematic because the property rights of the data as well as the utilization rights to the data may no longer rest with the original owner of the data. For commercial use, the United States is an insecure third country. Due to the EU Directive, data may technically not be delivered abroad. The Safe Harbor Agreement, existing since 2000 and reworked in 2005, is designed to prevent precisely this. The main goal of the Safe Harbor Agreement is to ensure that an adequate level of protection is imported in accordance with the Directive (Filip et al.2022)(Nissenbaum, 2020).

Entities that declare they will act in compliance with defined principles may then re-export data into the United States. The self-certification process, with the Federal Trade Commission responsible for enforcement, operates by means of declarations under penalty of perjury. According to the agreement, a corporation is compliant if it signs a statement of the Chief Executive Officer and the statement is legally binding on the company. If corporations violate the agreement, fines and penalties may result. The agreement ensures the safe passage of data of companies that voluntarily comply with the European set of agreed data protection standards. As a result, the self-certification has no legally sanctionable content. The agreement should protect European data from being tapped by American authorities because companies had agreed to the binding framework in question. The Safe Harbor Agreement has been criticized for being ineffective, and it was made conditional upon the reform in 2003 (Igbinenikaro and Adewusi2024)(Kreibich & Hermwille, 2021).

10. Conclusion and Future Trends

As the information and technology evolve and as computerized information systems become widespread, the need to ensure the protection of personal data, and not only this data, becomes particularly important. Given the high degree of concentration of personal data in computerized accounting programs, it is advisable to consider these valuable and privacy-sensitive resources as objects of particular threats or at least as newly emerged from the developed electronic environment that collects, processes, and uses them. Therefore, under these conditions, the establishment, development, and operation of a modern computerized accounting system should be carried out so

that information resources are effectively and reliably used, and the protection of basic principles for the protection of personal data is observed. The legislative framework determines the protection of personal data in computerized accounting programs, but also the prevailing accounting theory contributes to the establishment and development of a secure computerized accounting system (Marion and Fixson2021).

The future themes of the investigation could encompass the following new topics: the legislative framework for the protection of personal data in forces integrating the regulations on digital libraries and open science data; the presentation of the methodological approaches to provide scientific libraries with the information systems designed to process and analyze scientific visibility indicators; the scientific information evaluation models targeting the safety of personal data in big scientific data management with advanced protection measures; the criteria for the generation and use of scientific digital objects that are adequate in terms of personal data protection; the operational policies for scientific libraries designed to manage and preserve datasets with personal information; the development of a national repository for the preservation and use of scientific digital objects with particular attention to ensuring data privacy; the promotion of a sharing and trusted management model of personal data in the research and knowledge creation area; the identification of opportunities and evolution of blockchain technology at the base of platforms for the management and sharing of scientific research data in compliance with the privacy of personal data. Such themes ensure that scientific libraries collect, use, circulate, manage, and preserve personal data, thus playing an important role in a global scenario in which transparency and privacy will help realize the right of citizens to safeguard their personal data performance (ElMaraghy et al., 2021).

References

[1] Ahrens, T. & Ferry, L. (). Accounting and accountability practices in times of crisis: a Foucauldian perspective on the UK government's response to COVID-19 for England. Accounting. worktribe.com

[2] Ali, M. I., & Hussain, K. A. Unveiling the tapestry: a comparative investigation into data-protection legislation in India and Pakistan. Socrates. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law., 2024(1-28), 1-8. sciendo.com

[3] Akay, Ö. and Gündüz, F.F. (2022). Identification of factors affecting female labor force participation by panel var analysis: evidence from Turkey. Journal of Pure Social Sciences, 3(4), 12-26.

[4] Barati, M., Rana, O., Petri, I., & Theodorakopoulos, G. (2020). GDPR compliance verification in internet of things. IEEE access. ieee.org

[5] Bisbey, T. M., Kilcullen, M. P., Thomas, E. J., Ottosen, M. J., Tsao, K., & Salas, E. (2021). Safety culture: An integration of existing models and a framework for understanding its development. Human factors, 63(1), 88-110. sagepub.com

[6] Brown, J. S. & VanLehn, K. (2020). Towards a generative theory of "bugs". Addition and subtraction.

[7] Bulgakova, D. & Bulgakova, V. (2023). The compliance of facial processing in France with the article 9 paragraph 2 (a)(g) of (EU) general data protection regulation. ukma.edu.ua

[8] Cavoukian, A. (2021). Privacy by design: The seven foundational principles. IAPP Resource Center. thesedonaconference.org

[9] Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption. Sensors, 20(18), 5162. mdpi.com

[10] Daigle, B. (2021). Data protection laws in Africa: A pan-African survey and noted trends. J. Int'l Com. & Econ.. usitc.gov

[11] Deguchi, A., Hirai, C., Matsuoka, H., Nakano, T., Oshima, K., Tai, M., & Tani, S. (2020). What is society 5.0. Society, 5(0), 1-24. oapen.org

[12] Dokuchaev, V. A., Maklachkova, V. V., & Statev, V. Y. (2020). Classification of personal data security threats in information systems. T-Comm-Телекоммуникации и Транспорт, 14(1), 56-60. cyberleninka.ru

[13] ElMaraghy, H., Monostori, L., Schuh, G., & ElMaraghy, W. (2021). Evolution and future of manufacturing systems. CIRP Annals. sztaki.hu

[14] Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. Information Processing & Management.

[15] Faccia, A. & Petratos, P. (2021). Blockchain, enterprise resource planning (ERP) and accounting information systems (AIS): Research on e-procurement and system integration. Applied Sciences. mdpi.com

[16] Filip, R., Gheorghita Puscaselu, R., Anchidin-Norocel, L., Dimian, M., & Savage, W. K. (2022). Global challenges to public health care systems during the

COVID-19 pandemic: a review of pandemic measures and problems. Journal of personalized medicine, 12(8), 1295. mdpi.com

[17] Griffin, M., Martino, R. J., LoSchiavo, C., Comer-Carruthers, C., Krause, K. D., Stults, C. B., & Halkitis, P. N. (2021). Ensuring survey research data integrity in the era of internet bots. Quality & quantity, 1-12. springer.com

[18] Haque, A. K. M. B., Bhushan, B., & Dhiman, G. (2022). Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. Expert Systems. [HTML]

[19] Hasal, M., Nowaková, J., Ahmed Saghair, K., Abdulla, H., Snášel, V., & Ogiela, L. (2021). Chatbots: Security, privacy, data protection, and social aspects. Concurrency and Computation: Practice and Experience, 33(19), e6426. wiley.com

[20] Hasan, A. R. (2021). Artificial Intelligence (AI) in accounting & auditing: A Literature review. Open Journal of Business and Management. scirp.org

[21] Hossain, K. M. (2024). The Usefulness of an Accounting Information Systems for Effective Organizational Performance. Available at SSRN 4956574. ssrn.com

[22] Igbinenikaro, E., & Adewusi, O. A. (2024). Policy recommendations for integrating artificial intelligence into global trade agreements. International Journal of Engineering Research Updates, 6(01), 001-010. researchgate.net

[23] Kaissis, G. A., Makowski, M. R., Rückert, D., & Braren, R. F. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2(6), 305-311. nature.com

[24] Kaminski, M. E. (2021). The right to explanation, explained. In Research Handbook on Information Law and Governance (pp. 278-299). Edward Elgar Publishing. colorado.edu

[25] Korhonen, T., Selos, E., Laine, T., & Suomala, P. (2021). Exploring the programmability of management accounting work for increasing automation: an interventionist case study. Accounting, Auditing & Accountability Journal, 34(2), 253-280. tuni.fi

[26] Kreibich, N. & Hermwille, L. (2021). Caught in between: credibility and feasibility of the voluntary carbon market post-2020. Climate Policy. tandfonline.com

[27] Li, M., Wang, M., Fan, H., An, K., & Liu, G. (). A novel plaintext-related chaotic image encryption scheme with no additional plaintext information. Chaos.

[28] Marion, T. J., & Fixson, S. K. (2021). The transformation of the innovation process: How digital tools are changing work, collaboration, and

organizations in new product development. Journal of Product Innovation Management, 38(1), 192-215. sebastianfixson.com

[29] Murdoch, B. (2021). Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Medical Ethics. springer.com

[30] Müggenburg, H. (2021). Beyond the limits of memory? The reliability of retrospective data in travel research. Transportation Research Part A: Policy and Practice. [HTML]

[31] Nguyen, T. T., Huynh, T. T., Ren, Z., Nguyen, P. L., Liew, A. W. C., Yin, H., & Nguyen, Q. V. H. (2022). A survey of machine unlearning. arXiv preprint arXiv:2209.02299. [PDF]

[32] Nissenbaum, H. (2020). Protecting privacy in an information age: The problem of privacy in public. The ethics of information technologies. cpeterson.org

[33] Rahman, M. A., Hossain, M. S., Islam, M. S., Alrajeh, N. A., & Muhammad, G. (2020). Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. Ieee Access, 8, 205071-205087. ieee.org

[34] Ren, N., Zhu, C., Tong, D., Chen, W., & Zhou, Q. (2020). Commutative encryption and watermarking algorithm based on feature invariants for secure vector map. IEEE Access. ieee.org

[35] Solove, D. J. (2024). Murky consent: an approach to the fictions of consent in privacy law. BUL Rev.. ssrn.com

[36] Thapa, C. & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine. [PDF]

[37] Tsiligiris, V. & Bowyer, D. (2021). Exploring the impact of 4IR on skills and personal qualities for future accountants: a proposed conceptual framework for university accounting education. Accounting Education. tandfonline.com

[38] Turner, L., Weickgenannt, A. B., & Copeland, M. K. (2020). Accounting information systems: controls and processes. hoasen.edu.vn

[39] Vavoula, N. (2020). Interoperability of EU information systems: The deathblow to the rights to privacy and personal data protection of third-country nationals?. European public law. qmul.ac.uk

[40] Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear

elements of the proposed approach. Computer Law Review International, 22(4), 97-112. [PDF]

[41] Veit, R. D. (2022). Safeguarding regional data protection rights on the global internet—The European approach under the GDPR. In Personality and Data Protection Rights on the Internet: Brazilian and German Approaches (pp. 445-484). Cham: Springer International Publishing.

[42] Viljoen, S. (2021). A relational theory of data governance. Yale LJ. ssrn.com

[43] Vojković, G., Milenković, M., & Katulić, T. (2020). Iot and smart home data breach risks from the perspective of data protection and information security law. Business Systems Research: International journal of the Society for Advancing Innovation and Research in Economy, 11(3), 167-185. srce.hr

[44] Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. ACM Transactions on Management Information Systems (TMIS), 12(1), 1-20. researchgate.net

[45] Zhang, J., Fu, J., Hao, H., Fu, G., Nie, F., & Zhang, W. (2020). Root causes of coal mine accidents: Characteristics of safety culture deficiencies based on accident statistics. Process Safety and Environmental Protection, 136, 78-91.