TopHic | dig deeper

November 2021

# Will the Recovery and Resilience Plan boost Italian economy?

## Expert's Opinion

### *Recovery and Resilience Plan and Data Protection*

***Guglielmo Troiano***

*Manager Grant Thornton FAS*

The National Recovery and Resilience Plan (PNRR) Next Generation Italia is not just a project to help economic recovery, but primarily a unique occasion to overcome the dramatic effects of the pandemic period. The main target is to make Italy a greener, more digital and more resilient country, thanks to the availability of considerable financial resources and focusing on values related to the quality of individual life and on increased cohesion, inclusion and equity in the communities.
It is worth reminding that the Plan fits into a wider reform framework, aimed at regulating the European Union's technological innovation process. In fact, with the presentation of the Digital Service Act and of the Data Governance Act, the European Commission showed its willingness...

*read more*


## Overview

### *Recovery & Resilience Plan: opportunity and strategic choice*

***Giulio Tedeschi***

*Partner & Head of Advisory Bernoni Grant Thornton*

Professionals are currently busy with FY end activities and planning for 2022 and, as usual, have also to deal with the norms of the Budget Law, but this time also with the implementation of the National Recovery and Resilience Plan (PNRR). It is pointless to recall the opportunities the plan includes, as well as its strategic significance in business choices.
It is also true that the current planning on these topics also includes the agenda of activities...

*read more*

## Focus on

### *National Recovery and Resilience Plan and Cybersecurity*

***Alessandro Leone***

*Partner Grant Thornton FAS*

Cyber-attacks are on the rise globally, evidence of how significant and pervasive the skills and resources of those who have an interest in violating security systems are. Actually, both SMEs and bigger organisations, either public or private, better equipped and with more resources, are targeted by cyber-attacks, often successfully, which cause huge financial, but also - and most importantly - reputational damages.
A cyber-attack recently at the forefront of public debate is the one that last July targeted the IT systems of an Italian regional public administration. The attack highlighted various areas of improvement in the defence system.
It actually caused the interruption of a whole...

*read more*

*Supplemento Notizie flash n° 107 del 25 febbraio 1984*

# Overview

## *Recovery & Resilience Plan: opportunity and strategic choice*

***Giulio Tedeschi***
*Partner & Head of Advisory Bernoni Grant Thornton*

Professionals are currently busy with FY end activities and planning for 2022 and, as usual, have also to deal with the norms of the Budget Law, but this time also with the implementation of the National Recovery and Resilience Plan (PNRR).

It is pointless to recall the opportunities the plan includes, as well as its strategic significance in business choices.

It is also true that the current planning on these topics also includes the agenda of activities business, as well as professionals, plan to implement.

This issue of TopHic focuses on certain - among the various - issues above, to raise clients' awareness and help them make the correct choices.

The National Recovery and Resilience Plan originates from the need to develop a nationwide investment plan for the modernisation of the economy and the technological development is among the crucial areas (reference is often made to Italians' lack of familiarity with digital technologies), accompanied by structural investments and reforms aimed at activating the necessary processes for the modernisation and broadening of infrastructures and production chains.

One of the key elements of the Recovery and Resilience plan is Italy's digital evolution, to be achieved both through dedicated investments in the Public Administrations and through tax benefits and incentives to the private sector for investments in technology and IT consultancies.

A first consideration on digital evolution is related to personal data protection and the compliance with EU Regulation no. 2016/679, known as GDPR. It is sometimes said that this regulation is not "up to date" since it allegedly tries to limit the development of technology and the ability to analyse data accrued thanks to the latter. This is evidently a big mistake. In fact, the contrary is true. It is just because automations are now able to analyse huge quantities of data finding correlations among them that and outlining individuals' attitudes and behaviours that a regulation is now necessary to put order and to protect the individuals' fundamental rights. The Expert's Opinion analyses how to combine the advantages of the data analysis offered by digital evolution in compliance with the regulation.

On the other hand, digital evolution gives rise to another risk: that of cybersecurity. It can actually be easily inferred that if, on the one hand, there are growth opportunities linked to the adoption of IT systems, on the other hand, their vulnerability to cyber-attacks represents a huge risk for information confidentiality and for the continuation of normal operations. For this reason, cybersecurity is a priority for our government and it should be so also for Public Administration entities and private sector businesses. This topic is analysed in more detail in the Focus On section.

It is also worth recalling the increasingly felt need to address strategic choices - and the subsequent operations - towards a transition to circular economy.

The Recovery and Resilience Plan also includes a series of well-known necessary reforms required by Europe, as discussed almost on a daily basis on the media - so we are not going into details here - which essentially concern the reform of the Public Administration, of justice, of the promotion of competition and, last by not least, the simplification of legislation.

As concerns the latter topic, the tax reform included in this simplification process is now beginning to take shape with the approval of the relevant enabling law.

Much has already been said on the review of the land and buildings registry and on the necessary reduction of the tax burden as concerns workers' tax wedge and IRAP (regional production tax) taxation.

I would focus, instead, on the much-needed simplification of tax regulations, procedures and fulfilments. All this necessarily requires an organic rewriting of the regulation, currently consisting of confusedly scattered norms often hardly matching. This is the methodological approach underlying the draft enabling law based on which the Government will "embark upon the revision of the norms". Of course, this approach leads to the obvious and desirable hypothesis of having a consolidated text on tax law containing all the norms organised by homogeneous areas, combined with the equally important aim of obtaining a simplified tax regulation.

The draft law codifies these shared methodological principles and art. 9 of the draft enabling law actually refers to un update aiming at simplifying language. It actually underlines the need to "coordinate under the formal as well as substantial profile the text of the law provisions currently in force, including those transposing and implementing the EU regulation, introducing adequate amendments to guarantee an improved juridical, logical and systemic consistency of the regulation" and thus to safeguard "the uniqueness, completeness and clarity of the regulation of each sector".

Professionals dealing with the tax regulatory "jungle" on daily basis will immediately understand how this latter principle does not simply represent a general statement, but fits in a reasonable and shared need to be enabled to apply the regulation and comply with it, to knowingly manage a delicate and important area such as the tax one with an approach aimed at an "aware tax risk management".

Another area of the tax reform worth mentioning is the one relevant to the principle under art. 3, letter d) of the draft enabling law concerning the goal to harmonise the savings taxation regimes "also keeping into consideration the goal to contain tax elusion".

The reference to the term "elusion" strengthens the importance for taxpayers to have a clear and easily applicable regulation. The uncertainties which often have to be dealt with are often overwhelming, in particular with reference to financial income and investments and may imply the risk above, due complex interpretations which lead to tax litigations.

In such a sensitive area as savings, also protected by the Constitution, it is unthinkable that the uncertainty on the scope of the relevant norms leads to adjustments of the taxable income when the taxpayers' behaviour is led by a tax elusion intent.

The case of "financial" income (technically income from capital or property and capital gains) is actually one of those cases on which a regulatory intervention with the tax reform would be welcome.

It is actually necessary to eliminate any incompatibility between income from capital or property (e.g. proceeds, interest and dividends, but also periodic proceeds from investment and capital gains on some investment funds) and income currently classified as "other income" (e.g. capital gains originating from the difference between a financial instrument's sale and purchase price). This is still within the scope of asset management, an area in which the current regulatory inconsistency generates misunderstandings besides undermining taxpayers' trust with incomprehensible oddities which also impact the management of investments.

There are many examples of the inconsistencies above that asset management professionals have to deal with on a daily basis. The tax reform could therefore be the occasion to eliminate these differences and harmonise taxation regimes, not just in terms of consistency for common investors, but also in terms of regulatory uniformity (including the tax levy), with the additional benefit of reducing the risk of tax practices which the draft law rightly aims to eliminate.

The introduction of a single taxation regime, harmonised and consistent for all types of financial investments would help reach a full law compliance, safeguarding savings investments and thus helping to sustain the Italian economy and SMEs, making it less appealing to invest abroad. Therefore, this topic does not only concern taxation.

As far as corporate income is concerned, the first aspect on which the tax reform draft law focuses is the review of IRAP tax (i.e. the regional production tax). A further simplification would of course be welcome, but it is necessary to wait and see the approach which will be adopted by the legislator before commenting on the operational aspects.

Moving on to discuss corporate tax, art. 4, point 3b of the draft enabling law provides for a simplification and rationalisation of IRES (corporate income tax) aimed at reducing administrative fulfilments for companies, also through a focus on the harmonisation between statutory and tax values, with specific reference to amortisations and depreciations.

The topic is surely noteworthy, mainly for the welcome improved consistency between income resulting from the statutory financial statements and income for tax purposes (the recently amended provision under art. 83 of TUIR - income tax consolidated text - on the derivation of the corporate income taxable basis from the financial statements, according to which the correct application of the accounting principles issued by the competent settlors prevails also on the qualification, time-based recognition and classification criteria contained in TUIR).

The reform is commendable as it will allow to amend the delicate topic of the recognition of amortisations and depreciations, reviewing for tax purposes the regime contained in the decree issued in 1988 and never updated, which obviously does not take into account the technological development underwent by corporate assets.

The intervention in this area should also concern the methods used to determine the corporate income through increases and decreases, to adjust the regulation to the changes occurred in the economic system, aligning it to the norms in force in the main European countries, also in order to increase Italy's competitiveness on an international level. This harmonisation will also help reduce tax elusion, consistently with the lawmaker objectives.

A further area of intervention included in the draft law is the improvement of tax collection efficiency. This is an objective which will have an impact for taxpayers, starting from the overcoming of the premium on the collection (after the Constitutional Court warning in 2021). The enabling law aims to attain increased efficiency promoting the use of cutting-edge technology and the interconnection of databases with systems functional to the tax collection activity (art. 2 of the draft enabling law).

The other areas covered by the draft enabling law and not analysed in detail here concern income taxation for Irpef (personal income tax) purposes, amendments to some direct taxes, including VAT and amendments to municipal and regional supplementary taxes.

The above within the scope of a "reform" which should not impact on the public budgetary positions (art. 10 of the draft enabling law). A reform should probably consist of an organic and rational review of the regulatory framework, without impacting the budgetary positions. The reduction in taxation cannot, generally speaking, be implemented through provisions that politicians have to develop further with other provisions.

We started from the National Recovery and Resilience Plan to comment shortly on three of the various aspects which will guide professionals' strategic behaviours in the near future in order to seize the opportunities connected with the implementation of the plan. Generally speaking, we considered how the modernisation will be attained through the digitalisation and a transition towards a green circular economy, specifically through (i) cybersecurity, (ii) digital transformation and (iii) tax reform.

The above cannot happen without a step change, required to each professional to navigate this challenge. The importance of research cannot be underestimated, as it is no longer to be considered a cost centre, but rather as an essential asset for the strengthening and implementation of innovative models apt to improve skills and thus to ease the transition towards an economy increasingly based on know-how, as well as to devise lines of intervention covering the whole innovation, research and technological development process through the sharing of knowledge and skills of qualified workers.

Grant Thornton Italy's professionals are aware of the above trends and can help seize the opportunities connected to this challenge thanks to their skills, refined with their commitment to research, which is the necessary professional background to offer a wide range of services and keep on collaborating with clients starting from the areas analysed in this issue of TopHic.

We are dynamic consultants who offer integrated professional services, rather than just completing engagements, trusted providers and global advisors involved in the development processes that clients are devising and developing.

# Expert's Opinion

## *Recovery and Resilience Plan and Data Protection*

***Guglielmo Troiano***
*Manager Grant Thornton FAS*

The National Recovery and Resilience Plan (PNRR) Next Generation Italia is not just a project to help economic recovery, but primarily a unique occasion to overcome the dramatic effects of the pandemic period. The main target is to make Italy a greener, more digital and more resilient country, thanks to the availability of considerable financial resources and focusing on values related to the quality of individual life and on increased cohesion, inclusion and equity in the communities.

It is worth reminding that the Plan fits into a wider reform framework, aimed at regulating the European Union's technological innovation process. In fact, with the presentation of the Digital Service Act and of the Data Governance Act, the European Commission showed its willingness to define new paradigms to strengthen the internal digital service market.

"Mission 1: Digitalisation, innovation, competitiveness, culture and tourism" of PNRR aims at building momentum for the relaunch of Italian competitiveness and productivity. Such a huge challenge requires a far-reaching intervention, leveraging on various key elements of the Italian economic system to attain innovation, sustainability and a promotion of Italy's image and brand.

Next Generation EU's boost to the digital revolution will nonetheless lead to an inevitable and exponential increase in personal data processing, which will have to comply with the key GDPR principles. Therefore, all private and public entities intending to benefit from the advantages available under the PNRR will necessarily need to have completed, or at least have started, the adjustment process to reach full compliance with the personal data protection regulation, which is essential for digital innovation.

The Italian Data Protection Authority intervened on this point, drawing attention on the dual purpose of the protection provided by the GDPR within the scope of the reform project under the National Recovery and Resilience Plan: on the one hand, instilling confidence in citizens with reference to the activity of public entities when performing their functions and, on the other hand, guaranteeing the innovation process' security and thus increasing competitiveness without limiting individual rights and freedoms.

On the occasion of the presentation of the Council's annual report, the Italian Data Protection Authority emphasised that the only possible way to complete the Missions under the PNRR is the implementation of an effective synergy between Data Protection and Cybersecurity, since only the combination of these two factors can guarantee not only the attainment of an effective digitalisation and innovation process without threatening the security of the Country - currently safeguarded by the National Cybersecurity Framework - but also the safeguard of individual citizens' dignity.

The Authority also underlined the key importance of a dialogue between institutions and the Authority itself within the scope of the planning and implementation of the reforms. Thanks to its independence, the Authority can provide precious advice and meaningful ideas to help balance contrasting interests, such as technological progress and the safeguard of individual rights and freedom.

In addition, besides complying with GDPR principles, it will be necessary to exercise care and pay particular attention to the guarantees offered by providers and sub-providers, specifically Over The Top (OTT) players providing cloud technologies and artificial intelligence services.

On this point, the Recovery and Resilience Plan expressly mentions the so-called cloud first strategy: Public Administrations will have the possibility to choose whether to migrate to a new cutting-hedge national cloud infrastructure (National Strategic Hub, in Italian Polo Strategico Nazionale or PSN) or to a public secure solution, keeping into due consideration the type and volume of personal data processed and the type of services offered.

The digitalisation of the Public Administration (PA) is one of the top priorities of the Recovery and Resilience Plan. To achieve this objective, various measures have been devised, aimed at guaranteeing citizens and businesses higher quality, more efficient and innovative public services.

The digital infrastructures, both in the private and public sector, actually play a key role for most daily activities of the citizens and represent the backbone of the digital service system the Public Administrations use and offer to citizens and businesses. Guaranteeing Italy's technological autonomy, in a moment in history when most national interests are digital, is mandatory as well as instrumental to guarantee the control over the security of citizens' data, increasing meanwhile the resilience of digital services.

In the light of the above, the correct identification of all providers involved in the supply chain is essential, also when considering the transfer of personal data towards Extra EU Countries. Judgement no. C-311/18 by the Court of Justice of the European Union[1], also known as "Schrems II" imposed to all public and private organisations to reflect upon their compliance strategies, thus altering the balance of the global digital ecosystem. The abovementioned judgment will inevitably impact also on the enforcement of the PNRR, cloud computing being a vital technology for Italy's effective digitalisation process and to guarantee the actual provision of a homogeneous level of services to citizens nationwide.

The European Data Protection Supervisor (EDPS) recently undertook analyses[2] aimed as assessing the compliance of the contracts entered into by European Institutions with two of the main US Cloud Services OTTs - i.e. Amazon Web Services (AWS) and Microsoft - with the principles of the Schrems II judgement. According to the EPDS opinion, transfers of personal data to the US are particularly critical.

In the light of the above and upon due consideration of the importance cloud computing will have in the future for the development of State infrastructure, the EDPS deemed it advisable to devise a European strategy for the transfer of personal data by public entities, focused on a risk-based approach and on accountability - a great novelty for the GDPR - as well as on the collaboration between national Authorities and Public Administrations.

In this context, GDPR certifications will acquire specific importance, as they will allow holders to prove the attainment of a level of compliance able to increase the trust of users, clients and providers, giving a clear indication of the positive outcome of their adjustment process visible to third parties.

Finally, the Public Administration's digitalisation strategy, advocated in the Recovery and Resilience Plan, provides a major investment for the interoperability of databases. The aim is to improve the quality of the services offered, leveraging on the PA's wealth of information, whose use has often been characterised by serious inefficiencies due to a lack of coordination among the various public administrations. This scenario, as you may guess, always translated into further costs and red tape for both citizens and businesses.

In order to find a solution to this issue, the investment contained in the PNRR involves the creation of a National Digital Data Platform (Piattaforma Digitale Nazionale Dati or "PDND") on which each public entity may share and make information available through a list of digital interfaces (Application Programming Interface or "API").

The interoperability of databases will lead to a significant reduction in management costs and time necessary for data sharing, often rather significant due to the over-bureaucratisation characterising Public Administration processes. Citizens and businesses will be able to access public services based on the "once-only" e-government principle, according to which users have to provide their information to authorities and administrations "once-only", thus sharing on a single occasion all information necessary to the various interested administrations. To this end, the Agency for Digital Italy (Agenzia per l'Italia Digitale or "AGID") will adopt Guidelines and define technical criteria and technological standards for the management of the National Digital Data Platform, as well as the process for authentication and use of API resources.

As far as the impact of this system on personal data is concerned, the Italian Data Protection Authority already expressed its favourable opinion on 8 July 2021[3], acknowledging that AGID has defined a framework of guarantees and measures aimed at ensuring the integrity and confidentiality of personal data, often particularly sensitive, exchanged between databases, complying with the privacy by design and privacy by default needs, as set forth by the GDPR obligations.

In conclusion, the Digitalisation mission within the National Recovery and Resilience Plan (PNRR) guarantees incentives and tax credits to businesses for IT products and for programming, consultancy and related services.

This boost will encourage businesses in the private sector to undertake their path towards digitalisation. The trends recorded so far actually reveal, also in the private sector, the adoption of cloud computing, the introduction of artificial intelligence algorithms, Internet of Things or IoT, Robotics Process Automation or RPA, as a driver to perform low-value added routine activities, thus requalifying personnel for higher-value added activities.

Also in this case, it will be crucial to define suitable privacy by design and privacy by default processes, identifying the need to process personal data, specifying the relevant aims and identifying the correct legal bases legitimising the processing, in compliance with the fundamental GDPR principles.

Subjects processing data will need to be identified and authorised with specific instructions or, if external, proceeding with the examination of the necessary appointments as data controller. Particularly important will be the identification of the entire supply chain, so as to have control over the data processing.

Particularly important for cloud services, but not just for them, is the identification of the places where data are processed, in order to apply the correct guarantees for possible transfers outside the European Economic Area.

The evolution of digitalisation needs to be supported by a concurrent evolution of cybersecurity measures, which, in any case, may introduce some issues related to the potential control of remote workers. A careful analysis of the balance of interests should lead to adequate management procedures, to be agreed upon with the authorised subjects, in compliance with the provisions of the Workers' Statute.

Moreover, as concerns the evolution of digitalisation, specific attention will have to be paid to algorithms which may affect the data subjects' fundamental rights, such as those able to make autonomous decisions on data subjects or those performing profiling aimed at identifying attitudes or behavioural habits. In such cases, the impact on the data subjects' rights needs to be carefully evaluated, without prejudice to the compliance with GDPR principles, assessing the various methodologies and defining the correct protection measures. And without forgetting that data subjects have the right not to be subject to decisions based only on automated processing: to this end, it will be extremely important to inform them about their right to require a human intervention and to adopt the necessary procedural provisions to guarantee them the right to object the decision.

[1] *Court of Justice of the European Union (CGUE), Judgement no. C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, 16 July 2020, https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX:62018CJ0311.*

[2] *https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en.*

[3] *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9682994.docweb-display/docweb/9682994.*

## Focus on

### *National Recovery and Resilience Plan and Cybersecurity*

*di* ***Alessandro Leone***
*Partner Grant Thornton FAS*

Cyber-attacks are on the rise globally, evidence of how significant and pervasive the skills and resources of those who have an interest in violating security systems are. Actually, both SMEs and bigger organisations, either public or private, better equipped and with more resources, are targeted by cyber-attacks, often successfully, which cause huge financial, but also - and most importantly - reputational damages.

A cyber-attack recently at the forefront of public debate is the one that last July targeted the IT systems of an Italian regional public administration. The attack highlighted various areas of improvement in the defence system. It actually caused the interruption of a whole regional system, as the direct practical consequence was the disruption of the entire regional services network, including the vaccination management system, with non-negligible recovery times ranging from days up to whole weeks, also in the better equipped organisations.

According to some studies, in Italy the total cost for businesses and citizens for cyber-attacks in 2021 will be equal to approx. 6,000 billion dollars[4].

Moreover, as specified by the Minister for technological innovation, V. Colao, almost 95% of public administration servers are subject to the risk of cyber-attacks. And yet, cybersecurity is often considered by organisations as a cost they can do without, rather than an investment. On the contrary, it is clear that improvements to the IT systems security would imply a lower cost compared to value of the risk of a cyber-attack, with loss of data or the disruption of normal operations.

Technological innovation and digital transition in the last few years have been expanding constantly and quickly, thus contributing to focus the concept of business competitiveness on the ability to adopt cutting hedge technological solutions and to develop new applications to make operations easier and quicker, to increase efficiency and reduce costs. Therefore, in order to achieve these targets, it is necessary to plan a solid cybersecurity strategy, i.e. the practice to protect systems, networks and programs from cyber-attacks, which are usually aimed at the unauthorised access, change and dissemination of sensitive data or at the interruption of business operations[5]. Cybersecurity operates crosswise on various protection levels and is based on the integration of people, processes and technologies to build a robust defence and guarantee confidentiality, integrity and availability of information (so-called CIA Paradigm).

The Italian cyber security regulatory framework includes various interventions aimed at outlining a final architecture still under construction. On 16 December 2020 the Commission published the EU Cybersecurity Package, a collection of regulations, directives, guidelines and policies on cybersecurity; among these are in particular EU Directive no. 2016/1140 (NIS Directive) and EU Regulation no. 2019/881 on ENISA (EU Cybersecurity Act). The NIS Directive is the first actual legislative document on cybersecurity and it represents a centralised intervention aimed at attaining a minimum common level of security for networks and IT systems in Europe; it was implemented in Italy with Legislative Decree no. 65/2018. The main requirements, in line with the need of centralising and coordinating information on incidents and cyber vulnerabilities, are the identification of a single point of contact at a domestic and European level for the cooperation with NIS Authorities and with the European Commission, and the creation of a sole incident response centre through a Computer Security Incident Response Team (CSIRT).

ENISA, i.e. the European Union Agency for Cybersecurity aims at guaranteeing a high and effective level of network and information security and at promoting the establishment of a cybersecurity culture for the benefit of European citizens, consumers, businesses and public sector organisations to guarantee the functioning of the internal market. The main tasks performed by ENISA are: i) the collection of appropriate information to analyse the current and emerging risks relevant to the digital world for the European institutions and the Member States Authorities; ii) the facilitation of the cooperation between the Commission and the Member States for the development of common methodologies to prevent, identify and solve network and information security issues; iii) the tracing of the development of standards for products and services dedicated to the security of networks and information.

Generally speaking, the cybersecurity national governance framework is delegated to national security bodies, which are called upon not only to perform an information activity through digital systems, but also to intervene with a view to prevention, response and resilience.

In Italy, cybersecurity still needs to be addressed with a structured approach, but it is on the agenda of political decision makers also as concerns the implementation phase of the National Recovery and Resilience Plan, which includes sixteen topics grouped into six macro missions, among which is digital transformation. With reference to this area, the Plan identifies three overall targets: the digitalisation of the Public Administration, the innovation of the Public Administration and the organisational innovation of the judicial system. Achieving the digital growth and modernisation targets is a priority for Italy's recovery and relaunch. Moreover, the digitalisation of Public Administration systems and services has now become a topic that can no longer be postponed in order to change citizens' and businesses' perception and make PA a true 'ally' - to recall the term used in the Recovery and Resilience Plan - able to drastically reduce distances and thus bureaucracy-related timing between public entities and individuals.

This is yet truer in the light of the 'forced' transition to remote work made necessary by the Covid-19 pandemic which hit the Italian economy more than other EU Countries and which revealed the delays accumulated by the Public Administration.

The PA digitalisation process is based first of all on the allocation of 620 million Euros and is structured into seven investment areas, among which is cybersecurity.

The first area of intervention includes digital infrastructures with the adoption of a cloud first approach based on which Public Administration progressively need to abandon own IT infrastructures to adopt cloud technology. This measure became necessary since PA's data centres do not ensure a suitable level of cyber security. The Agency for Digital Italy (AGID), in charge of coordinating the PA digitalisation, structured the cloud first strategy based on three guidelines which they can choose to follow with reference to the infrastructures towards which to migrate: 1) infrastructures offered by authorised private Cloud Service Providers (CSPs) indicated by AGID in specific registers; 2) Community Cloud infrastructures for which public service contracts have been entered into by CONSIP; 3) infrastructures made available by the National Strategic Hub (PSN).

The second area of intervention focuses on a support and incentive program for cloud migration in the technical analysis and priority-setting phase, aimed in particular at local administrations.

The third investment measure concerns data and interoperability and tries to achieve the target of PA's digital transformation by changing the design and interconnection methods between databases in order to have a shared and universal access to data, following the "once-only" principle, according to which information should be required to citizens only once, with a consequent reduction in times and costs related to their input. To this end, the Recovery and Resilience Plan set forth the need to create a National Digital Data Platform (PND) accessible through a dedicated service compliant with GDPR privacy requirements, eliminating the need for citizens to provide the same information to various administrations more than once.

The fourth investment is aimed at strengthening and improving the efficiency of digital services and digital citizenship through a wider diffusion of PagoPA[6] (a system to simplify payments in favour of Public Administrations) and of the IO[7] app, the introduction of new digital services also in the mobility sector and an integrated action to improve the user experience of digital services. The broadening of the digital scope makes organisations still more vulnerable to cyberattacks, since the data collected and processed are the most profitable target for intruders, as[8] the average value of a medical record sold on the dark web is approx. 1,000 US Dollars. Therefore, the legislator deemed it advisable to dedicate the fifth scope of intervention exclusively to cybersecurity, starting from the implementation of the regulation on "National Cybersecurity Perimeter".

In particular, investments reserved to cybersecurity are divided into four areas of intervention:

1. strengthening of front-line control systems for the management of alerts and detected at-risk events targeted against PAs and national interest companies;
2. building and/or strengthening of the technical skills for the evaluation and the ongoing audit of the security of electronic devices and applications used by entities carrying out vital functions to provide critical services to citizens;
3. hiring of new personnel for both the public security and criminal investigation police forces, dedicated to the prevention and investigation of cybercrimes targeted against individual citizens, and the forces dedicated to protect the Country from cyberattacks;
4. consolidation of assets and cyber units in charge of the national protection and security and response to cyber threats.

The sixth area of intervention focuses on the digitalisation of big central administrations and includes various aspects of PA, such as for example Justice, Labour, Defence, Internal Affairs and Tax Police.

The last area of intervention concerns the improvement of citizens' basic digital skills, in order to support the digital literacy process.

Moreover, for the purposes of this article, it is worth mentioning the legislator's intent to digitalise, innovate and maintain competitiveness in the manufacturing system through investments in ultrafast 5G optic fibre connections. The latter are a key condition for the realisation of the gigabit society and to allow companies to make use of various 4.0 technologies (such as sensors, Internet of Things or IoT, 3D printers[9]). The internet connection and the various interconnections between devices on the one hand lead to various benefits in terms of real-time interaction with data, but on the other hand they increase inevitably the perimeter of cyberattacks. And while experts work to prevent and manage cyberattacks in dynamic contexts, there is one element beyond their control: the human factor, i.e. the users' behaviour when using devices. The first true protection is the compliance with the users' best practices, which can range from a correct management of passwords and access credentials and a careful management of suspect emails to the connection to a safe network and the physical safety of devices.

As a final note, the Digitalisation mission within the National Recovery and Resilience Plan allocates incentives and tax credits to businesses for IT products and IT planning, consultancy and related services. This boost will lead businesses in the private sector to undertake a quick path towards digitalisation. The trend registered so far actually testifies, also in the private sector, the adoption of cloud computing, the introduction of artificial intelligence algorithms, the adoption of the Internet of Things or IoT, the evolution of Robotic Process Automation or RPA, as drivers for the performance of routine or low-value added activities, with the resulting opportunity to requalify personnel for higher-value added activities.

In this context, cybersecurity plays a key role to safeguard IT assets and to sustain future developments, both in Public Administration and in the private sector.

In many cases, public entities and private sector businesses still need, to date, to identify the roles and responsibilities related to the management of cybersecurity and to structure a specific management process. In particular, it is necessary to define a risk analysis process allowing to align investments in cybersecurity with strategic objectives, involving the entire chain of command. It is therefore crucial to regulate all key cybersecurity processes: the management of IT accesses so that information can be accessed by authorised people only, seeing also to restrict their access only to necessary information; the management of physical accesses to the premises and to equipment rooms; the management of assigned personal IT devices; the classification of information and the relevant protection; the definition of the correct backup and recovery procedures, as well as the procedures for operational continuity, and so on. Adequate security measures also need to be identified (by way of example: firewalls, SIEM, antivirus/ end point protection, etc.) to safeguard the infrastructure, as well as projects to improve cybersecurity through an ongoing reassessment.

As a final note, a good cybersecurity management process needs to include risk and performance indicators with alarms and risks monitoring processes, also in real time, in order to be able to promptly respond to threats.

---

[4] *'Cyber Security, approccio sistemico e sostegno alle PMI, Il Sole 24 Ore, 18 agosto 2021 di E. Ferretti.*

[5] *CISCO.*

[6] *Payment platform between PA and citizens and businesses, under the PNRR.*

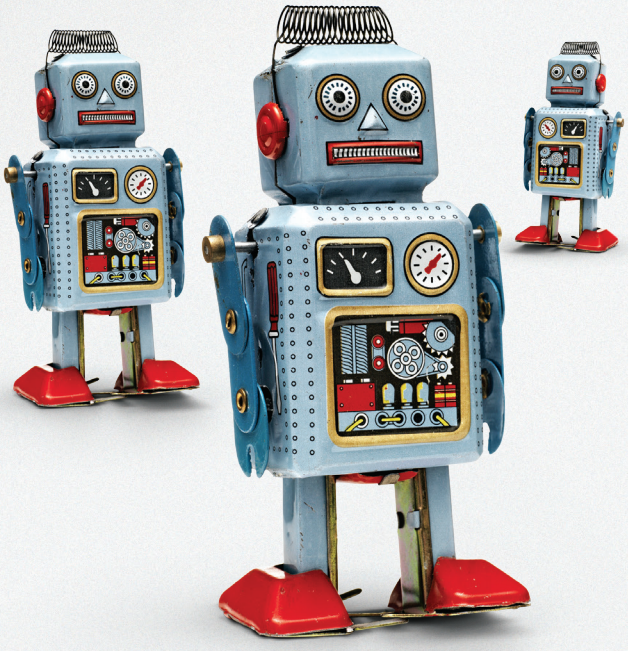
[7] *Versatile front-end/ channel aiming at becoming the single access point for all PA digital services.*

[8] *"Attacchi hacker, dati sanitari in pericolo: la lista segreta dei 35 ospedali colpiti", Corriere della Sera, di M. Gabanelli e S. Ravizza, 28 settembre 2021.*

[9] *Classificazione ripresa dal PNRR.*

STATUS QUO IS ONE OF MANY.

Audit | Tax | Advisory



**Status Go**™

IS ONE-ON-ONE.

Ready for an approach that's as unique as it is personal?

***Welcome to Status Go.***

**grantthornton.global**

Grant Thornton