LEADING BY EXAMPLE

THE EDPS STRATEGY 2015-2019

EDPS

European Data Protection Supervisor

THE EDPS STRATEGY

2015-2019

LEADING BY EXAMPLE

ABOUT THIS DOCUMENT

This is a crucial moment for data protection, a period of unprecedented change and political importance, not only in the EU but globally. In this context, the new European Data Protection Supervisor (EDPS) has finalised a strategy for the next five years to turn his vision into reality and to identify innovative solutions quickly.

This 2015-2019 Plan summarises:

- the major data protection and privacy challenges over the coming years;
- three strategic objectives and 10 accompanying actions for meeting those challenges;
- how to deliver the strategy, through effective resource management, clear communication and evaluation of our performance.

Our aims and ambitions build on our strengths, successes and the lessons learned from implementing our *Strategy 2013-2014: Towards Excellence in Data Protection*.

ABOUT US

The European Data Protection Supervisor (EDPS) is a relatively new but increasingly influential independent supervisory authority, with responsibility for monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities to ensure consistent data protection.

The Supervisor, Giovanni Buttarelli, and Assistant Supervisor, Wojciech Wiewiórowski, were appointed in December 2014 by the European Parliament and the Council of the EU. Together with the basic requirement of independence, the EDPS remit[1] includes:

- developing and communicating an overall vision, thinking in global terms and proposing concrete recommendations and practical solutions;
- providing policy guidance so as to meet new and unforeseen challenges in the area of data protection;
- operating at the highest levels and developing and maintaining effective relationships with a diverse community of stakeholders in other EU institutions, Member States, non-EU countries and other national or international organisations.

The Supervisors are supported by the Office of the EDPS, a dynamic team of skilled and experienced lawyers, IT specialists and administrators which aims to serve as an impartial centre of excellence for enforcing and reinforcing EU data protection and privacy standards, both in practice and in law.

1 Vacancy notice for the European Data Protection Supervisor COM/2014/10354 (2014/C 163 A/02), OJ C 163 A/6 28.5.2014.

VISION, OBJECTIVES AND ACTION 2015-2019

The EDPS' vision is to help the EU lead by example in the global dialogue on data protection and privacy in the digital age. Our three strategic objectives and 10 actions are:

1. ***Data protection goes digital***

   (1) Promoting technologies to enhance privacy and data protection;
   (2) Identifying cross-disciplinary policy solutions;
   (3) Increasing transparency, user control and accountability in big data processing.

2. ***Forging global partnerships***

   (4) Developing an ethical dimension to data protection;
   (5) Mainstreaming data protection into international policies;
   (6) Speaking with a single EU voice in the international arena.

3. ***Opening a new chapter for EU data protection***

   (7) Adopting and implementing up-to-date data protection rules;
   (8) Increasing accountability of EU bodies collecting, using and storing personal information;
   (9) Facilitating responsible and informed policymaking;
   (10) Promoting a mature conversation on security and privacy.

THE EDPS' CORE VALUES

- **Impartiality** – working within the legislative and policy framework given to us, being independent and objective, finding the right balance between the interests at stake.
- **Integrity** – upholding the highest standards of behaviour and doing what is right even if it is unpopular
- **Transparency** – explaining what we are doing and why, in clear language that is accessible to all
- **Pragmatism** – understanding our stakeholders' needs and seeking solutions that work in practice.

CONTENTS

Giovanni Buttarelli, Supervisor (centre) and Wojciech Wiewiorowski, Assistant Supervisor (right), with Christopher Docksey, Director (left), acting together as the EDPS Management Board.

FOREWORD

This is truly an historic moment for data protection.

Over the last 25 years, technology has transformed our lives in positive ways nobody could have imagined. Big data, the internet of things, cloud computing, these have so much to offer to improve our lives. It is likely that big data will become even bigger, as better quality personal information becomes a requirement for effective analysis, in order to deliver results of increased value. But these benefits should not be at the expense of the fundamental rights of individuals and their dignity in the digital society of the future.

So big data will need equally big data protection.

Europe needs to be at the forefront of shaping a global standard for privacy and data protection, a standard centred on the rights and the dignity of the individual. The EU has a window of opportunity to adopt the future-oriented standards that we need, standards that inspire others at global level.

We can do this by leading by example, as a beacon of respect for digital rights. The EU is at its best when citizens and our international partners can see that our actions are consistent with what we profess to be our values. Europe has to lead the conversation on the legal and ethical consequences of these new technologies.

This means adopting the data protection reform this year. A modern, future-oriented set of rules is key to solving Europe's digital challenge. We need EU rules which are innovative and robust enough to cope with the growing challenges of new technologies and trans-border data flows. Data protection must go digital.

In the front line are the EU institutions and bodies who should lead the way in demonstrating accountability in practice. The EDPS will continue to be an active partner, providing the EU institutions with practical and dynamic solutions, so that this enhanced compliance will set an example to others.

Data protection will remain a relevant factor in most EU policy areas, and is the key to legitimising policies and increasing trust and confidence in them. We will help the EU institutions and bodies to be fully accountable as legislators, to build data protection into the fabric of their legislative proposals.

Of course, these are global concerns, not merely European issues. Data protection laws are national, but the data are not. And this means that Europe has to lead by example in building new global partnerships to develop common ground on basic principles. We need to invest in better dialogue with fellow regulators, industry and civil society to explore how to make international cooperation, particularly transatlantic agreements, fairer and more balanced in practice.

To achieve this, it is important to develop a single European voice on these strategic data protection issues. So we will work hard to support cooperation with fellow independent data protection authorities on these issues.

This new Strategy sets out what Wojciech Wiewiórowski and I plan to achieve, together with Christopher Docksey and our talented and dynamic colleagues in the Office of the EDPS. We hope to see the EDPS develop as a centre of interest for data protection, a forum for debate, and a place where all are welcome to work together on protecting our fundamental rights.

Giovanni Buttarelli

DATA PROTECTION IN THE DIGITAL ERA

Digital technology is an extraordinary catalyst for all forms of social expression and social change. From amusing videos and games to revolutions powered by social media, technology can enable the powerless to challenge the powerful. There is no doubt that technology brings many benefits, both individual and social.

As data protection regulators, we need to approach this with an open mind and identify the opportunities it will create for our societies in terms of prosperity, well-being and other significant benefits, particularly for important public interests.

On the other hand, the widespread collection and use of massive amounts of personal data which occurs today -made possible through cloud computing, big data analytics and electronic mass surveillance techniques- is unprecedented.

As a result, data protection is playing an increasingly central role in modern regulatory approaches for the world we live in. But while technical innovation races ahead, institutional reaction is slow.

In particular, this digital environment is determining:

- how people communicate, consume and contribute to social and political life in the post big data world;
- how businesses organise themselves to make profits;
- how governments interpret their duty to pursue public interests and protect individuals; and
- how engineers design and develop new technologies.

The way that we respond now to rapid change and challenges, including threats to security, will have consequences for us and future generations that inherit the digital world. This is an historic opportunity to open a new chapter for data protection in the digital era.

To benefit from new technologies and preserve the rights of the individual, the new EDPS aims to be an epicentre for creative ideas and innovative solutions, customising existing data protection principles to fit the global digital arena.

This innovative thinking relates to both the EU Digital Agenda and data protection principles. We do not need to reinvent these principles, but we do need to 'go digital'. We need to make existing principles more effective in practice in our technology-driven society and integrate them with some new principles specifically derived from the digital age and the big data driven economy.

THE INTERNATIONAL DIMENSION

Data protection laws are national, but personal information is not. As a result, the international dimension of data protection has, for years, been the subject of much debate. We have discussed intensively how we can better engage and achieve greater convergence on a global scale. These discussions have intensified over the last two years, since the first disclosures of mass surveillance. There has been a lot of good substance in these talks, but little practical action.

Data protection has to be taken into account across the broadest sweep of EU policies. It is a top policy priority. In cooperation with non-EU countries, Europe needs to be at the forefront in shaping a global, digital standard for privacy and data protection.

This standard should be centred on individuals, their rights and freedoms, and their personal identity and security.

In such a global scenario, a clear and modern, future-oriented set of rules is also the key to solving Europe's digital challenge.

The EDPS aims to help the EU to lead by example as a beacon of respect for fundamental rights.

We can turn the risks into an opportunity, to make the EU principles and best practices robust enough to effectively address the challenges of the big data world we will increasingly inhabit.

BIG DATA = BIG ACCOUNTABILITY

The popularity of the internet can largely be attributed to the way it has tapped into our social nature. Whether or not new products and technologies appeal to us, together with our desire to stay safe and not appear foolish, determines whether they will have mass appeal.

But the widespread collection of massive amounts of personal information is taking control of personal information away from individuals and limiting their ability to engage freely in the digital world.

Big data challenges regulators and independent authorities to ensure that our principles on profiling, identifiability, data quality, purpose limitation, and data minimisation and retention periods are effectively applied in practice.

Big data that deals with large volumes of personal information implies greater accountability towards the individuals whose data are being processed. People want to understand how algorithms can create correlations and assumptions about them, and how their combined personal information can turn into intrusive predictions about their behaviour.

This means giving clear information to them about:

- who is responsible for collecting and using the information;
- the purpose for doing so;
- what information is processed, whether it is knowingly volunteered by the individual, or whether it is observed and inferred without the individual's knowledge;
- how information is processed, including the logic used by algorithms to determine assumptions and predictions about individuals;
- how long the information will be stored and with whom it will be shared.

Digital technologies need to be developed according to data protection principles, giving more say to individuals on how and why their information can be used, with more informed choice where relevant. Data analytics are increasingly powerful but they remain prone to mistakes in the assumptions and biases they can make about individuals. Individuals must be able to challenge such biases, and they must be properly informed on how and why their information can be used. This means we must put an end to opaque privacy policies, which encourage people to tick a box and sign away their rights.

The future is inspiring and filled with untapped potential. Powerful online companies are serving up great opportunities, seemingly for free, for use in our day-to-day lives. But there is a cost. Digital technology is increasingly determining the way we live, placing sophisticated, pervasive, predictive and real-time software in the hands of a few powerful companies.

Our values and our fundamental rights are not for sale. The new technologies should not dictate our values, and we should be able to benefit both from new technologies and our fundamental rights.

Such concerns are not new: the first computers were greeted with a similar degree of apprehension. But with the perceived ubiquity of data, the global phenomena of cloud computing, big data analytics, the internet of things and techniques for electronic mass surveillance, these concerns have become more urgent than ever.

One solution is to assess the ethical dimension beyond the application of the data protection rules. Organisations, companies and public authorities that handle personal information are responsible for how that information is collected, exchanged and stored, irrespective of whether these decisions are taken by humans or algorithms. An ethical approach to data processing recognises that feasible, useful or profitable does not equal sustainable. It stresses accountability over mechanical compliance with the letter of the law.

We want to encourage a better informed conversation on what big data and the internet of things will mean for our digital rights. These are not only European issues but global concerns.

FORGING GLOBAL PARTNERSHIPS

Accountability in handling personal information is a global challenge.

An ethical dimension to data protection involves reaching out beyond the community of EU officials, lawyers and IT specialists towards thinkers who are equipped to judge the medium to long-term implications of technological change and regulatory responses.

We will work closely with our national colleagues to reinforce cooperation and encourage the EU to speak with one voice in the global fora on privacy and data protection matters.

As a data protection authority, we are able to draw on our experience of advising EU bodies on international transfers, on the design and operation of e-government services and on the supervision of large-scale IT systems.

We will invest in dialogue with IT experts, with industry and civil society to explore how to improve international cooperation, including arrangements for existing and future data-flows, in the interests of the individual.

We will also invest in global partnerships with fellow experts, non-EU countries, authorities and international organisations to work towards building a social consensus on principles that can inform binding laws and the design of business operations and technologies and the scope for interoperability of different data protection systems.

A NEW CHAPTER FOR EU DATA PROTECTION

The EU currently occupies a privileged position as the point of reference for much of the world on privacy and data protection. But for the EU to continue being a credible leader in the digital age, it must act on its own fundamental principles of privacy and data protection, and it must act quickly.

After many years of talk, the reform of the EU data protection rules is more urgent than ever. Society and technology will not wait for Europe to catch up with developments. The longer it takes to adopt a new set of rules, the greater the risk that they will be obsolete on implementation.

The reform should not slow down innovation, but equally it should ensure that our fundamental rights are safeguarded in a modern manner and made effective in practice, to rebuild the trust in the digital society that has been eroded not least by covert and disproportionate surveillance.

It is vital to make data protection easier, clearer and less bureaucratic, so that it will underpin the digital world now and into the future.

Though the current EU rules on handling personal information have served Europeans relatively well, the fragmented national approach to data protection is not sustainable. When EU Data Protection Directives were agreed in the 1990s, the internet was in its infancy and we had little idea of the impact it would have on society and the economy. A similar paradigm shift is about to take place now. Technologies will continue to develop in a manner that is unpredictable even for their designers.

Individuals, public authorities, companies and researchers now need a rulebook which is unambiguous, comprehensive and robust enough to last two decades and that can be enforced as required by the European and national courts as well as by truly independent data protection authorities. It needs to uphold the rights of the online generation growing up today.

The EDPS will be a more proactive partner in the discussions between the European Commission, Parliament and Council on the data protection reform, in particular in the final trilogue.We will

look for practical and workable solutions that avoid red tape and are flexible enough to accommodate technological innovation and cross-border data flows.

We will help legislators find pragmatic solutions to strengthen the roles of individuals and supervisory authorities, and the accountability of controllers, while simplifying existing formal requirements where necessary. Data protection needs to be more dynamic and less bureaucratic.

Judging by current trends, we may expect a century's worth of technological changes to occur between now and 2030, the likely duration of the reform. If the devil is in the detail, it is in some unnecessarily rigid details of certain provisions of the Reform. There is a risk that some of these provisions will become ineffective or obsolete before the full package is reviewed again. These provisions can be better tailored without lowering the level of the relevant safeguards, providing flexibility without ambiguity. The scalability of a certain number of obligations is also an issue.

In a modernised regulatory framework for the digital economy of the future, big data protection can be a driver for sustainable growth. A solid EU Digital Agenda can build on a solid foundation of modern data protection.

The EU should lead the way in applying principles to the new and emerging realities of how people communicate and do business.

Europe has 12% of the world's population, yet represents over 26% of the world's internet users. At the same time, only a fraction of the leading technology companies are European and the market for privacy-enhancing technologies is dwarfed by the market for data analytics.

The way Europe responds to the challenges it faces will serve as an example for other countries and regions around the world grappling with the same issues.

ACCOUNTABILITY OF EU BODIES

EU bodies, including the EDPS, must be fully accountable for how they process personal information, because to demonstrate exemplary leadership we must be beyond reproach.

Our aim is to leverage our expertise as a dynamic supervisory authority in advising the EU institutions on the reform of current rules to meet these global challenges. We want to raise the awareness of the relevance of data protection rules and principles and how to apply them in specific sectors, in practice and in policymaking.

We will strive for even better interaction with the EU institutions and bodies we monitor, with a view to becoming increasingly effective.

We aim to be more selective, intervening only where there are important interests at stake or interventions that can clearly lead to an improved data protection culture and encourage accountability within EU institutions, embedded as a part of their day to day good administration, not as a separate discipline.

We will continue to use our enforcement powers with discretion, seeking in the first place to ensure compliance by persuasion and example rather than by diktat, following the principle of accountability and encouraging the commitment of senior management in the EU institutions.

On the basis of our experience in implementing the data protection rules for EU institutions, as laid down in Regulation 45/2001, we will be proactive in our cooperation with the EU legislator to modernise them in parallel with the Data Protection Reform.

TIME FOR AN ENTIRELY NEW CONVERSATION ON SECURITY AND PRIVACY

Public security and combating crime and terrorism are important public objectives. However, unnecessary, disproportionate or even excessive surveillance by or on behalf of governments sows mistrust and undermines the efforts of lawmakers to address common security concerns.

The EU has struggled in recent years to identify effective measures in this policy area that do not excessively interfere with the fundamental rights to privacy and data protection; measures that are necessary, effective and proportionate. We know that threats to the security of our lifestyle and freedoms are real and may evolve. But how can we avoid the majority becoming the innocent victims? The priority should be a coherent and systematic mechanism for tracking the behaviour and movements of known criminal and terrorist suspects, not the indiscriminate collection of personal data.

Scrutiny of the necessity and proportionality of specific measures to fight crime and terrorism warrants a broad debate. These are principles enshrined in the Charter of Fundamental Rights as applied in the case law of the Court of Justice of the EU; high-level legal requirements of EU law that the EDPS is tasked with safeguarding. As an independent authority, the EDPS is not automatically for or against any measure; we are fully committed to our mission of advising the EU institutions on the implications of policies which have a serious impact on these fundamental rights. We are ready to work more closely with the legislator to find innovative legal and technological solutions.

We have to establish a clear and comprehensive set of principles and criteria which law enforcement and national security must respect when they interfere with our fundamental rights. We must do this by considering the Data Protection Reform as a package and by thinking about how existing and future bilateral and international agreements can work in a more balanced way.

OUR COMMITMENT

Our vision is for the EU to lead by example as a beacon of respect for data protection and privacy and to speak with a single, credible and informed voice on fundamental rights in the digital world.

An important part of our role is to explain the European approach to data protection simply and clearly and to ensure that its relevance is maintained amid rapid technological change.

In our supervision of EU institutions, we will act through education, persuasion and example, preserving our powers of enforcement as a last resort.

This strategy is a challenging and ambitious agenda for a small professional organisation. But we know we can rely on the skills of our experienced and motivated staff. With their support, we know we can achieve much more.

We are acutely aware that our effectiveness depends on constructive and active partnership, on common endeavour with our partner national data protection authorities and the Article 29 Working Party. When the European Data Protection Board is established, we will play the role established by the legislators effectively, facilitating and supporting informed dialogue among national authorities.

This strategy is our public commitment to achieving this vision over the next five years. It is a commitment to transparency, accountability and selectiveness in what we do.

We now have a unique chance to shape a global, digital standard for the respect of privacy and the protection of personal information.

It's time for data protection to go digital, because society has already done so.

THE ACTION PLAN

In addressing these issues, we have identified three strategic objectives and 10 priority actions to help us make the EU an exemplary leader in the digital age.

1. DATA PROTECTION GOES DIGITAL

ACTION 1

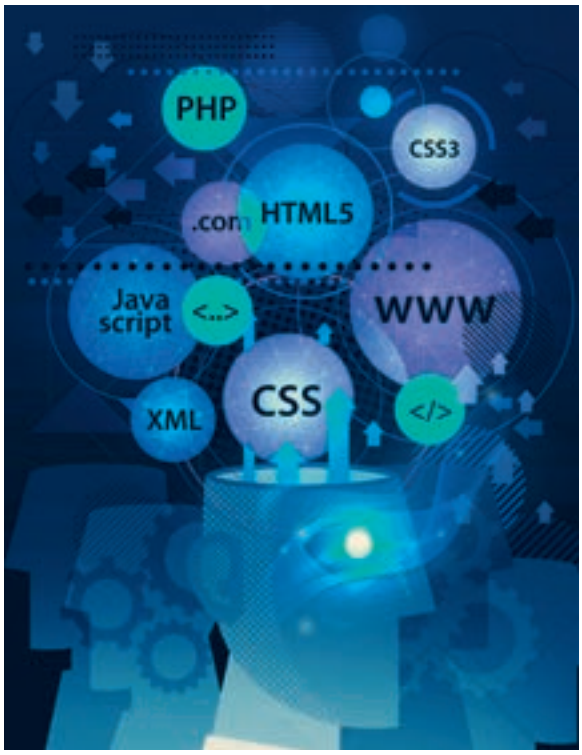
Promoting technologies to enhance privacy and data protection

- Work with communities of IT developers and designers to encourage the application of privacy by design and privacy by default through privacy engineering;
- Promote the development of building blocks and tools for privacy-friendly applications and services, such as libraries, design patterns, snippets, algorithms, methods and practices, which can be easily used in real-life cases;
- Expand the Internet Privacy Engineering Network (IPEN) to work with an even more diverse range of skill groups to integrate data protection and privacy into all phases of development of systems, services and applications;
- Provide creative guidance on applying data protection principles to technological development and product design;
- Highlight that data protection compliance is a driver for consumer trust and more efficient economic interaction, and hence can encourage business growth;
- Work with academia and researchers in the public and private sectors focusing on innovative fields of technical developments that affect the protection of personal data, in order to inform our technology monitoring activities.

ACTION 2

Identifying cross-disciplinary policy solutions

- Initiate and support a Europe-wide dialogue amongst EU bodies and regulators, academics, industry, the IT community, consumer protection organisations and others, on big data, the internet of things and fundamental rights in the public and private sector;
- Work across disciplinary boundaries to address policy issues with a privacy and data protection dimension;
- Initiate a discussion on broad themes which integrates insights from other fields, and coordinate training efforts to familiarise staff with these related disciplines.



ACTION 3

Increasing transparency, user control and accountability in big data processing

- Develop a model for information-handling policies, particularly for online services provided by EU bodies, which explains in simple terms how business processes could affect individuals' rights to privacy and protection of personal data, including the risks for individuals to be re-identified from anonymised, pseudonymous or aggregated data;

- Encourage the development of innovative technical solutions for providing information and control to users, reducing information asymmetry and increasing users' autonomy.

2. FORGING GLOBAL PARTNERSHIPS

ACTION 4

Developing an ethical dimension to data protection

- Establish an external advisory group on the ethical dimension of data protection to explore the relationships between human rights, technology, markets and business models in the 21st century;

- Integrate ethical insights into our day-to-day work as an independent regulator and policy advisor.

ACTION 5

Mainstreaming data protection into international agreements

- Advise EU institutions on coherently and consistently applying the EU data protection principles when negotiating trade agreements (as well as agreements in the law enforcement sector), highlighting that data protection is not a barrier but rather a facilitator of cooperation;

- Monitor the implementation of existing international agreements, including those on trade, to ensure they do not harm individuals' fundamental rights.

ACTION 6

Speaking with a single EU voice in the international arena

- Promote a global alliance with data protection and privacy authorities to identify technical and regulatory responses to key challenges to data protection such as big data, the internet of things and mass surveillance;

- Cooperate with national authorities to ensure more effective coordinated supervision of large scale IT systems involving databases at EU and national levels, and encourage the legislator to harmonise the various existing platforms;

- Maximise our contribution to discussions on data protection and privacy at international fora including the Council of Europe and the OECD;

- Develop our in-house expertise on comparative data protection legal norms.

3. OPENING A NEW CHAPTER FOR EU DATA PROTECTION

ACTION 7

Adopting and implementing up-to-date data protection rules

- Urge the European Parliament, the Council and the Commission to resolve outstanding differences as soon as possible on the data protection reform package;

- Seek workable solutions that avoid red tape, remain flexible for technological innovation and cross-border data flows and enable individuals to enforce their rights more effectively on and offline;

- Focus during the post-adoption period on encouraging correct, consistent and timely implementation, with supervisory authorities as the main drivers;

- In the event that the EDPS provides the Secretariat for the new European Data Protection Board (EDPB), allow this body to be ready on 'day one' in close cooperation with national colleagues, in particular by ensuring proper transitional arrangements are in place to enable a seamless handover from the Article 29 Working Party;

- Work in partnership with authorities through the EDPB to develop training and guidance for those individuals or organisations that collect, use, share and store personal information in order to comply with the Regulation by the beginning of 2018;

- Engage closely in the development of subsequent implementing or sector-specific legislation;

- Develop a web-based repository of information on data protection as a resource for our stakeholders.

ACTION 8

Increasing the accountability of EU bodies processing personal information

- Work with the European Parliament, Council and Commission to ensure current rules set out in Regulation 45/2001 are brought into line with the General Data Protection Regulation and a revised framework enters into force by the beginning of 2018 at the latest;
- Continue to train and guide EU bodies on how best to respect in practice data protection rules, focusing our efforts on types of processing which present high risks to individuals;
- Continue to support EU institutions in moving beyond a purely compliance-based approach to one that is also based on accountability, in close cooperation with data protection officers;
- Improve our methodology for inspections and visits, in particular a more streamlined method for inspecting IT systems.

ACTION 9

Facilitating responsible and informed policymaking

- Develop a comprehensive policy toolkit for EU bodies, consisting of written guidance, workshops and training events, supported by a network;
- Identify each year the EU policy issues with the most impact on privacy and data protection, and provide appropriate legal analysis and guidance, whether in the form of published opinions or informal advice;
- Increase our in-house knowledge of specific sectors so that our advice is well-informed and relevant;
- Establish efficient working methods with the Parliament, Council and Commission and actively seek feedback on the value of our advice;
- Develop our dialogue with the Court of Justice of the EU on fundamental rights and assist the Court in all relevant cases, whether as a party or an expert.

ACTION 10

Promoting a mature conversation on security and privacy

- Promote an informed discussion on the definition and scope of terms such as national security, public security and serious crime;

- Encourage the legislators to practically collect and examine evidence from Member States (in closed sessions if required) that require the collection of large volumes of personal information, for purposes such as public security and financial transparency, which would interfere with the right to privacy, to inform our advice to the EU legislator on necessity and proportionality;

- Promote convergence between the different laws on data protection in the areas of police and judicial cooperation, as well as consistency in the supervision of large scale IT systems. This should include the swift adoption of the draft Directive on the processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences.

DELIVERING THE STRATEGY

We aim to deliver our strategy through the careful management of our resources, clear communication and regular monitoring and evaluation of our performance.

EFFECTIVE RESOURCE MANAGEMENT

We intend to continue our strong record in planning and monitoring the spending of financial resources.

We will continue to manage and develop our staff in order to broaden our expertise and networks.

We will continue to work towards developing an agile, flexible and professional organisation. We will continue to prioritise our work rigorously and develop our strategic management of human resources.

We will develop and implement a total quality management system.

We will set the example of accountability and lead the way in how we ourselves handle personal information.

CLEAR COMMUNICATION

Data protection is often perceived as technical and obscure for non-experts. In order to correct this perception, we will use straightforward language to make technical issues more accessible.

In the interests of transparency, we are committed to communicating in clear and concise, jargon-free language, appropriate to our different audiences.

This applies to all our activities, whether opinions, guidance, website or interaction with the media, regardless of the complexity of the legal or technological matter in question.

MEASURING OUR PERFORMANCE

We will work in a transparent and accountable way, establishing our annual management plan, publishing our Annual Report and holding ourselves to a set of key performance indicators linked to the objectives of this strategy.

At the end of each year we will adopt a work programme for the following year which addresses the main priorities for data protection in the EU, organised according to the strategic objectives and priority actions.

The Annual Report will evaluate our progress against our overall objectives from the previous year, with particular reference to the key performance indicators (KPIs). The KPIs that were identified in January 2013 for the previous Strategy 2013-2014 will be reviewed over the course of the first year of the current strategy to assess whether they need to be adapted.

A fuller mid-term review of the strategy will be carried out in consultation with our stakeholders within the EU bodies and beyond. The results of the review will be included in the EDPS 2017 annual report, which we intend to publish in early 2018.

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*):

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the Internet (http://europa.eu).

Luxembourg: Publications Office of the European Union, 2015

Print	ISBN 978-92-9242-055-0	doi:10.2804/795471	QT-01-15-039-EN-C
PDF	ISBN 978-92-9242-051-2	doi:10.2804/35559	QT-01-15-039-EN-N

QT-01-15-039-EN-N

THE EUROPEAN GUARDIAN OF DATA PROTECTION

www.edps.europa.eu

@EU_EDPS

Publications Office

EDPS

EUROPEAN DATA PROTECTION SUPERVISOR