ISSN: 1977-9127

European Data Protection Supervisor

EDPS Newsletter

No. 42 | July 2014

IN THIS ISSUE

HIGHLIGHTS

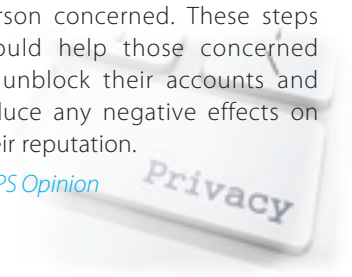
Bringing privacy in from the cold: asset freezing procedures at the Council

Asset freezing is one measure that can be taken against individuals suspected of certain serious crimes, such as terrorist activities, or human rights breaches committed by persons related to regimes in certain third countries. On the recommendation of member states, the European Council publishes lists of people whose assets should be frozen, together with the reasons, in the Official Journal of the European Union. Financial institutions are then obliged to block these accounts on the basis of these lists.

The EDPS was tasked with assessing the data protection implications of this process and, on 7 May 2014, we published our Opinion. In line with our approach from a previous *Opinion*, which addressed the asset freezing processing procedure used by the European Commission, we recommended that the Council limit the amount of information published in the lists. This would mean only publishing what is really necessary to identify the individuals concerned. In particular, we expressed our doubts concerning whether it is truly necessary to publish the reasons why someone is listed.

Occasionally, a person is found to have been listed in error. This usually happens as a result of a mistake or because the grounds for listing no longer exist. This presents a problem as, although the Council 'de-lists' those who are wrongly cited, the fact that they were ever on the list remains on public record in the Official Journal. To address this, we recommended that the Council not only correct the lists without delay and at regular intervals, but that it also takes additional measures to clear the names of those who are wrongfully listed. This could be done, for instance, by providing the reasons for erasure in the amending act, which is published in the Official Journal, or in a letter to the person concerned. These steps should help those concerned to unblock their accounts and reduce any negative effects on their reputation.

EDPS Opinion



Privacy and competitiveness in the age of big data

The collection and control of massive amounts of personal data are a source of market power for the biggest players in the global market for internet services, said the EDPS following the publication of our Preliminary Opinion on Privacy and competitiveness *in the age of big data: The interplay between data protection, competition law and consumer protection*. Personal information has become a form of currency to pay for so-called 'free' online services and is a valuable intangible asset for an increasing number of companies doing business in the EU. This requires closer interaction between different regulators.

The evolution of big data has exposed gaps in EU competition, consumer protection and data protection policies that do not seem to have kept up with this development. Smarter interaction across these partially overlapping policy areas will support growth and innovation and minimise the potential harm to consumers.

The EDPS is pleased to be facilitating discussions between regulators and experts in these fields.

Peter Hustinx, EDPS

EDPS Opinion

Your work emails, your personal data?

When a former EU staff member submitted a complaint to the EDPS concerning access to his professional email account, it was an opportunity for us to define what exactly should be considered as personal data in this context.

Our assessment of this issue followed the wide approach taken by the *Article 29 Working Party* on the concept of personal data. On this basis, the email address, the name of the staff member when mentioned in emails and attachments and the associated traffic information such as when an email was sent or received by a staff member, are all considered to be the personal data of the person concerned. The content of emails and associated attachments within an email account, however, should only be considered the personal data of a staff member if they relate to him as a data subject. For example, this might include emails on evaluation, work contract related issues and internal investigations or procedures concerning the staff member, as well as the staff member's personal assessment of certain situations or conduct.

However, just because someone has a right of access to personal data does not mean that they are automatically entitled to receive copies of entire documents or e-mails. The action to be taken will depend on the circumstances: sometimes it will be necessary to provide a copy of the documents, but in other situations it might be more appropriate, for instance, to give direct access to them on the premises of the EU institution or body - which qualifies under the EU Data Protection *Regulation* as *'communication in an intelligible form'*.

Establishing a definition for personal data

On the same theme as above, we adopted a decision in a complaint against the European Anti-Fraud Office (OLAF). The complainant alleged, among other things, that OLAF had not fully respected his right of access.

In dealing with the complainant, OLAF had applied a limited interpretation of Article 2 of *Regulation 45/2001*. The EDPS, however, considers that Article 2 of the Regulation specifies a much broader concept of personal data. Indeed, according to Article 2(a) of the Regulation, personal data is "any information relating to an identified or identifiable natural person."

This definition clearly refers to more than just the name of an individual. Once again, we drew on the approach set out by the *Article 29 Working Party (WP29)* to support our decision. The WP29 clarifies that information "relating to" an individual, in the sense of Article 2(a), includes information concerning the identity, characteristics or behaviour of an individual; information used to determine or influence the way in which that person is treated or evaluated; and data that, if used, is likely to have an impact on that individual's rights and interests. In light of this definition of personal data, the EDPS therefore requested that OLAF reconsider the answer it originally provided to the complainant's access request.

Data protection principles v. data conservation

Whilst conducting an internal investigation at another European institution, investigators from the European Anti-Fraud Office (OLAF) requested the records of professional phone calls made from the professional mobile phone of the person under investigation. It transpired that several years' worth of data were available. However, under the EU Data Protection *Regulation*, the storage of such data for more than six months is not permitted, unless it is required for a court matter that is already pending at the end of this period.

In the consultation, we were asked to consider whether these records could still be made available to OLAF. Given the fact that the retention of these documents was already unlawful, we advised that the records must not be provided to the investigators, but should be destroyed, along with any other communication records retained by the institution for more than six months. We also advised the institution concerned to put in place a system to ensure that retention periods are not exceeded in future. In response, both recommendations were implemented by the institution.

CONSULTATION

The EU should ensure an area of freedom, security and justice with the rights of individuals at its core

The EDPS has called on the European Council to place the rights of individuals at the core of justice and security policies in the years to come. The intention of the European Council to define strategic guidelines under the current treaties, for further legislative and operational planning in the area of freedom, security and justice is an opportunity to revitalise the EU's approach in these areas and to repair the loss of trust resulting from the revelations about mass surveillance. In his Opinion on the future development of the area of freedom, security and justice, the EDPS highlights the need for fuller integration of privacy and data protection in the activities of all EU institutions.

> ***The European Court of Justice's recent annulment of the data retention directive as an excessive violation of individuals' rights to personal data protection should serve as a wakeup call to the EU. Policymakers need to apply proper limitations and safeguards in a more informed and systematic manner when launching proposals which have a significant impact on fundamental rights.***
>
> Peter Hustinx, EDPS

EDPS Opinion

EDPS letter to Mr. Herman VAN ROMPUY, President of the European Council

Job-hunting made easy (and privacy friendly)

The EURES job mobility portal provides information, guidance and recruitment services to job-seekers throughout the EU. Job-seekers are able to upload their CV to the EURES database and search and apply for jobs, whilst employers are able to search for CVs which match their job openings. EURES is currently undergoing changes which will increase the capability of the portal to automatically match job vacancies with job applications. While this is good for job-seekers, it carries an increased privacy risk. For this reason, the European Commission has proposed a new Regulation which is designed to update the portal's legal framework and better protect job-seekers' data.

In our Opinion of 3 April 2014, we welcomed that the Commission proposal requires explicit consent from the workers concerned and takes due account of their right to access and correct their data. However, we also suggested that the proposal should specify more clearly who can access the database, what safeguards are in place to prevent abuse of the system and how the process of automated matching works. We advised that the Regulation should specify that those searching the EURES portal will not have direct access to an applicant's name, CV or any other directly identifiable personal data unless a worker chooses to make their entire CV available on EURES. We recommended that the purpose of any processing of data and the acceptable range of activities within which the data stored on EURES can be used be clearly specified.

EDPS Opinion

A strategy for keeping trade secrets safe

In its efforts to encourage economic growth, create a competitive job market and provide high-quality products and services in the EU, the European Commission launched its *Single Market for Intellectual Property Rights* strategy in 2011. As part of this, in late 2013, the Commission adopted a proposal for a Directive on the protection of trade secrets from unlawful acquisition, use and disclosure, on which the EDPS was consulted.

In this proposal, the concept of trade secrets or 'business information' is described as something which 'extends beyond technological knowledge to commercial data such as information on customers and suppliers' - which includes personal data.

The Commission proposal focuses on the rights of the person who holds the trade secret. It aims to establish a sufficient and comparable level of redress across the internal market, designed to counter the misuse of trade secret information, whilst also providing sufficient safeguards against abusive behaviour. In doing so, the proposal is intended to attract and retain investors and to boost confidence in the competitiveness of European companies. To comply with the Directive, member states would be required to put in place certain measures to protect secret information which is held lawfully by natural or legal persons.

In our Opinion of 12 March 2014, we focused on the obligations of a trade secret holder who is responsible for processing personal information (data controller) towards the individuals whose data s/he is responsible for (data subjects). Among other things, we recommended that:

- the relationship between personal data and the concept of trade secrets be defined;
- trade secrets and business secrets be clearly distinguished;
- the application of other EU legislation be further clarified; and
- the proposed directive should in no way infringe upon the rights of EU citizens, particularly their right to access the data being processed.

EDPS Opinion

Striking a balance between privacy and international security

The EU-US Terrorist Finance Tracking Program (TFTP) is used to gather intelligence and prevent terrorist attacks through the sharing of information about financial transactions between the EU and the USA. *Article 11 of the EU-US TFTP* commits the European Commission to carrying out a study on the possible introduction of an EU system equivalent to the TFTP, the TFTS (Terrorist Finance Tracking System), which would allow for a more targeted transfer of data from the EU to the USA. Under this system, the EU would have more control over its citizens' data than the current agreement, which is considered by many to put EU citizens' data at risk.

The impact assessment conducted by the Commission regarding the creation of the TFTS - a legal and technical framework for the extraction of data on EU territory - contains an analysis based on the principles of necessity, proportionality, cost-effectiveness and the safeguarding of fundamental rights. Taking all of this into account, the Commission has concluded that "the case to present at this stage a proposal for an EU TFTS is not clearly demonstrated".

In our formal comments of 17 April 2014, we welcomed this conclusion and the reasoning behind it. However, we drew attention to the fact that the Commission should have used the same analysis when assessing whether to continue, amend or terminate the EU-US TFTP agreement and we highlighted the need for a full analysis to be carried out. In the wake of last year's surveillance revelations, which led many to question the reliability and security of the TFTP agreement once again and in light of the recent data retention decision of the Court of Justice of the European Union (Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*), which found Directive 2006/24/EC invalid, this is particularly relevant.

Regarding the impact assessment, we were disappointed that the analysis did not include a more thorough investigation of the other options available to the EU in place of a TFTS. Nor did it take into consideration the conclusions of the reports of the *Joint Supervisory Body (JSB)* of Europol on its inspections

regarding implementation of the Agreement, nor the *Article 29 Working Party* analysis on the massive nature of transfers of financial data from the EU to the US and the limits of effective judicial and administrative redress. Addressing these issues is vital if the EU is to develop a better approach.

EDPS Comments

EDPS urges ICANN to limit collection and retention of personal data

The Internet Corporation for Assigned Names and Numbers (*ICANN*) initiated a public consultation on data collection and retention within the context of its 2013 Registrar Contract. The contract is designed to encourage accountability and transparency in the domain name industry, constituting a signed agreement between ICANN and registrars, who are the owners of domain names.

In our response of 17 April 2014, the EDPS encouraged ICANN to take the lead to ensure that when new tools, instruments or internet policies are designed, privacy and data protection are embedded in them by default (privacy by design) for the benefit of all – not only European - internet users. We advised ICANN that the Registrar contract should only require 'by default' the collection of personal data which is genuinely necessary for the fulfilment of the contract between the registrar and the registrant - such as for billing - or for other compatible purposes such as fighting fraud related to domain name registration. In addition, this data should not be retained for longer than is necessary for these purposes, nor for any other purposes, such as law enforcement or the enforcement of copyright.

EDPS Comments

New direction for traffic information services

Between December 2013 and March 2014, the European Commission conducted a public consultation on EU-wide real-time traffic information services. These services provide road users with helpful and timely information on things such as traffic regulations, driving routes, estimated travel times and potential delays to a journey. The public consultation aimed to gather stakeholders' views in an attempt to establish what problems there are with current services, identify opportunities for improvement and prepare specifications and standards for the future provision of these services.

In our formal comments of 12 March 2014, we stressed that the collection and use of real-time traffic information may entail the processing of personal data. This is particularly relevant when dealing with equipment such as the eCall platform or GPS, where information is collected from users. We therefore recommended that the Commission should take EU data protection law fully into account when implementing any future specifications or legislation in this area, in particular Directive 95/46/EC and Directive 2002/58/EC. To do this, the Commission must ensure that the concept of privacy is embedded in the IT infrastructure and software at the design stage (privacy by design). There must also be appropriate safeguards governing the collection and re-use of location data and we reminded the Commission that the EDPS should be consulted prior to the adoption of any new specifications in this area.

EDPS Comments

A modern internet governance model should be universal and respectful of fundamental freedoms

The efforts of the EU to build an integrated model of internet governance and data protection should be complemented by an effective reform of the EU's own legal framework and the swift adoption of the General Data Protection Regulation, said the EDPS following the publication of his Opinion on the Commission Communication on Internet Policy and Governance – Europe's role in shaping the future of Internet Governance.

EDPS Opinion

EDPS Press Statement

The EDPS: advising the EU institutions on policy and legislation

The EDPS has produced a new policy paper explaining how we advise the EU institutions on policy and legislation. Specifically, it takes into account the major changes in the legal, economic and technological context that have occurred since 2004, when our institution was established, in particular, the entry into force of the Lisbon Treaty, as well as a number of landmark decisions handed down by the European Court of Justice which have underlined the importance of privacy and data protection as an integral part of EU decision making.

Under Article 28(2) of the data protection Regulation, the Commission has an obligation to consult the EDPS whenever it adopts a legislative proposal which relates to the protection of individuals' rights and freedoms in the processing of personal data. The scope of this obligation is broad as, in line with established practice, the EDPS is also consulted *informally* before such proposals are adopted by the Commission.

In order to maximise the impact and usefulness of our work, we are developing a 'policy toolkit', which includes general guidance for the legislator through, for instance, thematic or sectorial guidelines. The toolkit is designed to help the institutions make informed decisions on the data protection impacts of new proposals.

Policy Paper

COURT MATTERS

Google ordered to comply with 'right to be forgotten'

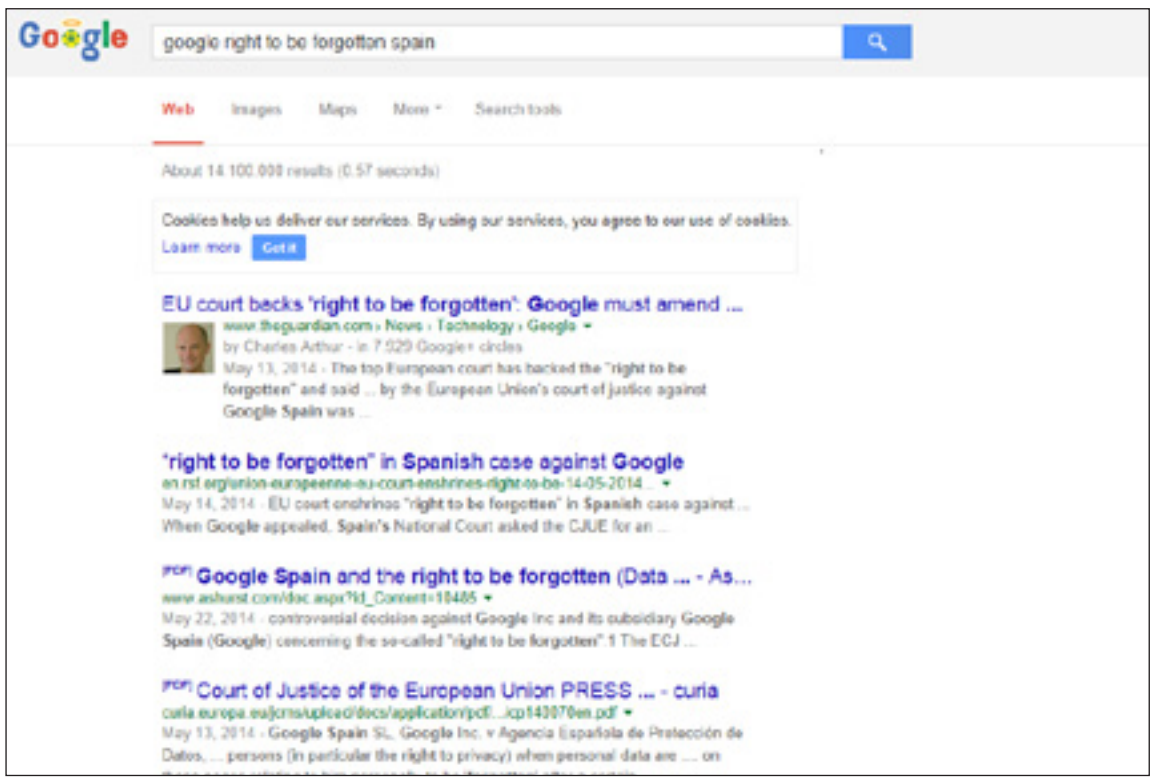
On 13 May 2014, the Court of Justice of the European Union once again delivered a very important judgment. This case involved interpreting a number of key provisions in the Data Protection Directive 95/46/EC in the context of a claim by an individual, Mr. Costeja Gonzalez, who requested that his personal data be removed from a results list published by the Google search engine.

Firstly, the Court clarified that the activity of an internet search engine does indeed constitute the "processing of personal data" and that the operator of such a search engine is a responsible data *controller*. Secondly, the Court decided on the applicability of the data protection Directive to companies based in third countries (such as the USA) which are operating in the EU through a branch or subsidiary. In this case, the Directive was considered applicable since the activities of Google Inc. (the search engine) and Google Spain (which is responsible for the promotion and sale of advertising space) were "inextricably linked". Finally, on the so-called "right to be forgotten", the Court ruled that individuals have the right to ask for their data to be erased – based on both the right to erasure and the right to object, which are both provided for in the Directive – not only if their personal information is inaccurate, but whenever the processing does not comply with the provisions of the Directive. Such requests can be made directly to the search engine.

The European data protection authorities assembled in the WP29 will now analyse the ruling and provide guidelines, in order to develop a common approach to the implementation for the ruling across the EU.

Judgment

WP29 Press Release



Court of Justice judges EU Data Retention Directive invalid

On 8 April 2014, the Court of Justice of the European Union delivered its judgment in joined cases C-293/12, C-594/12 *Digital Rights Ireland* and *Seitlinger and Others*. In a landmark decision (for which the EDPS was invited by the Court to provide input at the hearing) the Court declared the Data Retention Directive 2006/24/EC invalid.

The ruling highlights the value placed on the fundamental right to privacy which is at the very core of EU policy. Indeed, it is the first time an entire Directive was invalidated solely on the basis of its incompatibility with the EU Charter of Fundamental Rights. It also sets clear limits on any blanket government surveillance of communications data (or 'metadata'). In particular, the Court underlined that data retention constitutes a serious and unjustified interference with the fundamental right to privacy enshrined in Article 7 of the EU Charter of Fundamental Rights. When an EU act imposes obligations which interfere with this right, the EU legislature must provide the necessary guarantees and not leave this responsibility entirely to the Member States.

The judgment also means that the EU should take a firm position in discussions with third countries, particularly the USA, regarding access to and use of the communications data of EU residents.

Judgment

Attacking the heart of internet privacy

In April of this year, a serious vulnerability, the Heartbleed bug (CVE-2014-0160), was discovered in OpenSSL, a popular encryption tool used to provide security and privacy for internet communications. In the vulnerable versions of OpenSSL, the Heartbleed bug makes it possible to read and access data that should be protected. This leaves internet applications, such as emails, instant messaging, web surfing and Virtual Private Networks (VPNs) open to exploitation and possible theft of personal data.

The vulnerability has been included in versions of OpenSSL since 2012. The vulnerable functions were also part of many popular software packages, including some commercial games and office software.

Given its extensive and serious impact, the security community at large reacted swiftly to the bug. Internet services such as Wikipedia, Yahoo and Amazon all seemed to be vulnerable and appeared to take the necessary measures to quickly fix the bug on their systems. The European institutions also took measures to ensure that their services would not be attacked. Users of affected services were advised to change their passwords and the certificates used for encrypting internet traffic between affected websites were replaced. In reaction to the incident, the *Linux Foundation* created a new initiative, aimed at improving the quality of security checks for widely used open source software. Yet despite all these measures, it is possible that there are servers which have not yet been updated and which are therefore still using the affected software.

Heartbleed represents a serious threat to individuals' privacy, whilst also demonstrating the vital importance of ensuring that the computer and internet systems used to process personal data are properly secure.

Engineering privacy: the IPEN Initiative

Edward Snowden's revelations of mass internet surveillance triggered a debate among internet engineers, who see it as their responsibility to *safeguard the personal data and privacy* of internet users (page 4 of EDPS newsletter 40). In response, several remarkable projects have been launched, aimed at improving security and privacy protection for internet users. The Internet Privacy Engineering Network (IPEN), launched by the EDPS in collaboration with national DPA's, academics and engineers, is one such project. It is designed to serve as a platform for the cooperation and exchange of ideas between Data Protection Authorities (DPAs) and internet engineers.

The purpose of IPEN is to close the gap between technical tools (guided by engineers and IT experts) and personal data protection needs (guided by the law) by encouraging the development of privacy friendly solutions for common engineering problems and enabling developers to recognise when their technical choices have an impact on privacy principles.

IPEN aims to build a network of privacy experts from the technical, developer and policy communities. This network will work together on three main tasks:

- To share information about on-going initiatives and projects addressing privacy-related development needs;
- To identify *'use cases'* - where tech engineers identify a series of steps that will enable them to solve a specific problem - for which privacy can be implemented at the design level; and,
- To launch projects for the development of tools and building-blocks which enable and enhance privacy.

In addition, IPEN will build a repository of relevant resources, making its findings and knowledge base accessible to all participants, developers and privacy experts.

Thus far, IPEN has been presented at a number of events and has garnered support from 'hackers', open source developers, internet and web engineers, academic researchers and developers, as well as experts in national DPAs.

For more information or to get involved in the IPEN initiative, please contact *ipen@edps.europa.eu*

EVENTS

Privacy, Consumers, Competition and Big Data

On 2 June 2014, the EDPS hosted a workshop to discuss the links between the EU's approach to competition, consumer protection and data protection against the rapidly evolving backdrop of the digital economy.

Experts from academia, think tanks and legal practice from both sides of the Atlantic were joined by EU and national policy makers and regulators in looking at various themes explored by the EDPS in our *Preliminary Opinion* published on 26 March 2014, including the assessment of market power and dominance, the consumer welfare interest and the potential for abuse and exploitation in sectors where personal data is traded as a currency in exchange for 'free' services, often without the consumer being fully aware of the transaction. Keynote speeches by a former and a present FTC Commissioner brought a US perspective on issues which are increasingly shared as a result of the global and borderless nature of the 'big data ecosystem'.

Discussions confirm that the different policy areas employed separate lexicons but had more in common than one might think at first. The EDPS was pleased to help give a boost to the conversation between opinion formers from a variety of disciplines. There was a clear consensus on the need to continue to identify gaps and synergies, and to start identifying what action is needed and by whom.

It was a closed session conducted under the Chatham House rule to enable frank and honest discussion.

A fuller report on the event will be published in the coming weeks.

DATA PROTECTION OFFICERS

The next issue of EDPS newsletter will be online in the autumn. Enjoy the summer!

French and German versions of this newsletter will be online shortly.

SPEECHES AND PUBLICATIONS

- Speaking points (*PDF*) delivered by Giovanni Buttarelli at Inet 2014, "Internet: Privacy and Digital Content in a Global Context", Istanbul (21 May 2014)
- "Restoring Trust across the Atlantic", article (*PDF*) by Peter Hustinx published in "TELOS, Revista de Pensamiento sobre Comunicación, Tecnologia y Sociedad" (2 May 2014)

About this newsletter

This newsletter is issued by the European Data Protection Supervisor (EDPS) – an independent EU authority established in 2004 to:

- monitor the EU administration's processing of personal data;
- give advice on data protection legislation;
- cooperate with similar authorities to ensure consistent data protection.

You can subscribe / unsubscribe to this newsletter via our website.

CONTACTS

www.edps.europa.eu
Tel: +32 (0)2 2831900
Fax: +32 (0)2 2831950
NewsletterEDPS@edps.europa.eu

POSTAL ADDRESS

EDPS
Rue Wiertz 60 – MTS Building
B-1047 Brussels
BELGIUM

OFFICE ADDRESS

Rue Montoyer 30
B-1000 Brussels
BELGIUM

Follow us on Twitter: @EU_EDPS

EDPS - The European guardian of data protection

QT-AC-14-002-EN-C doi:10.2804/62174 ISBN 978-92-95073-01-2