



VIRTUAL & AUGMENTED REALITY TOOLKIT TO ENGAGE SENIORS BRAIN WITH
INTER-GENERATIONAL UNDERSTANDING

ERASMUS+ PROJECT

Intellectual Output 3: An Empowering Guide to Exploiting AR/VR with Seniors

Chapter 6

**Legal skills and legal organization form, risk
management, privacy and security**

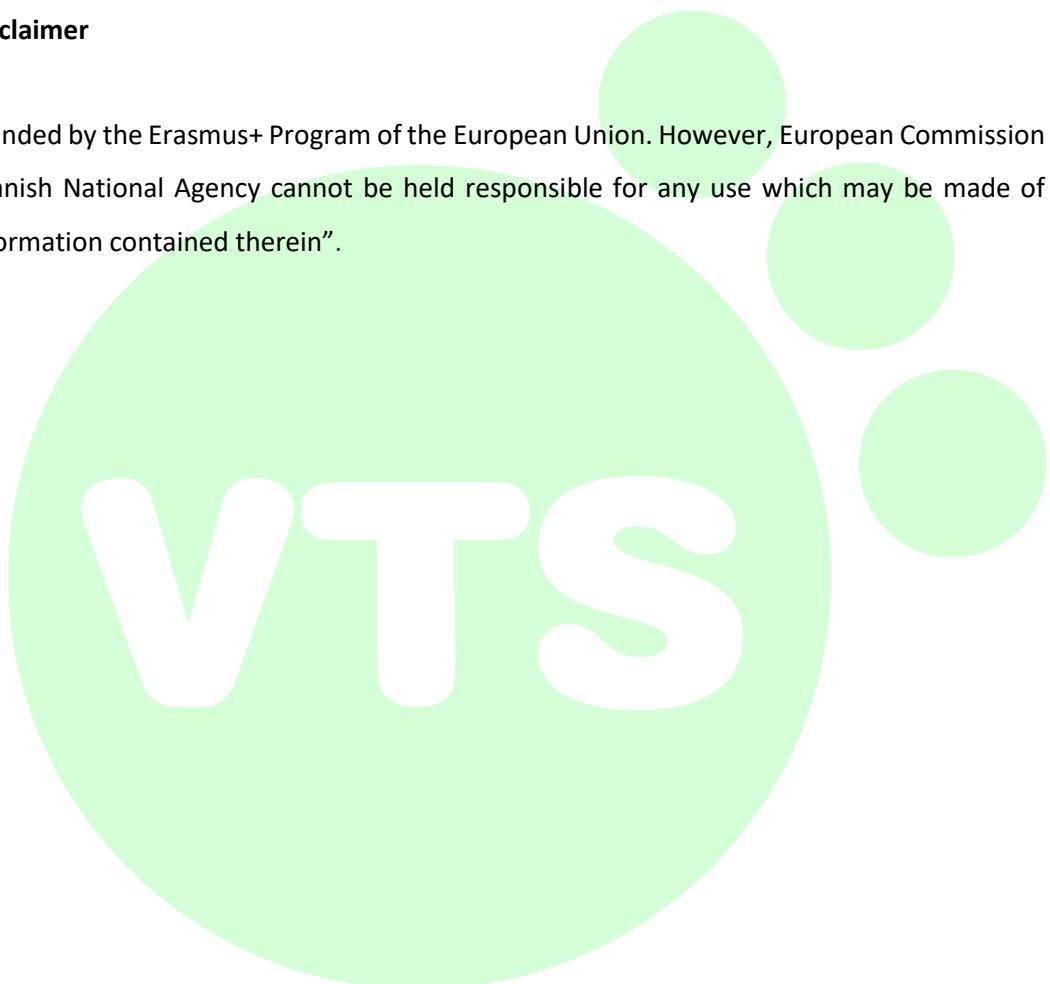
Co-funded by the
Erasmus+ Programme
of the European Union



PROJECT NUMBER – 2020-1-ES01-KA204-082270

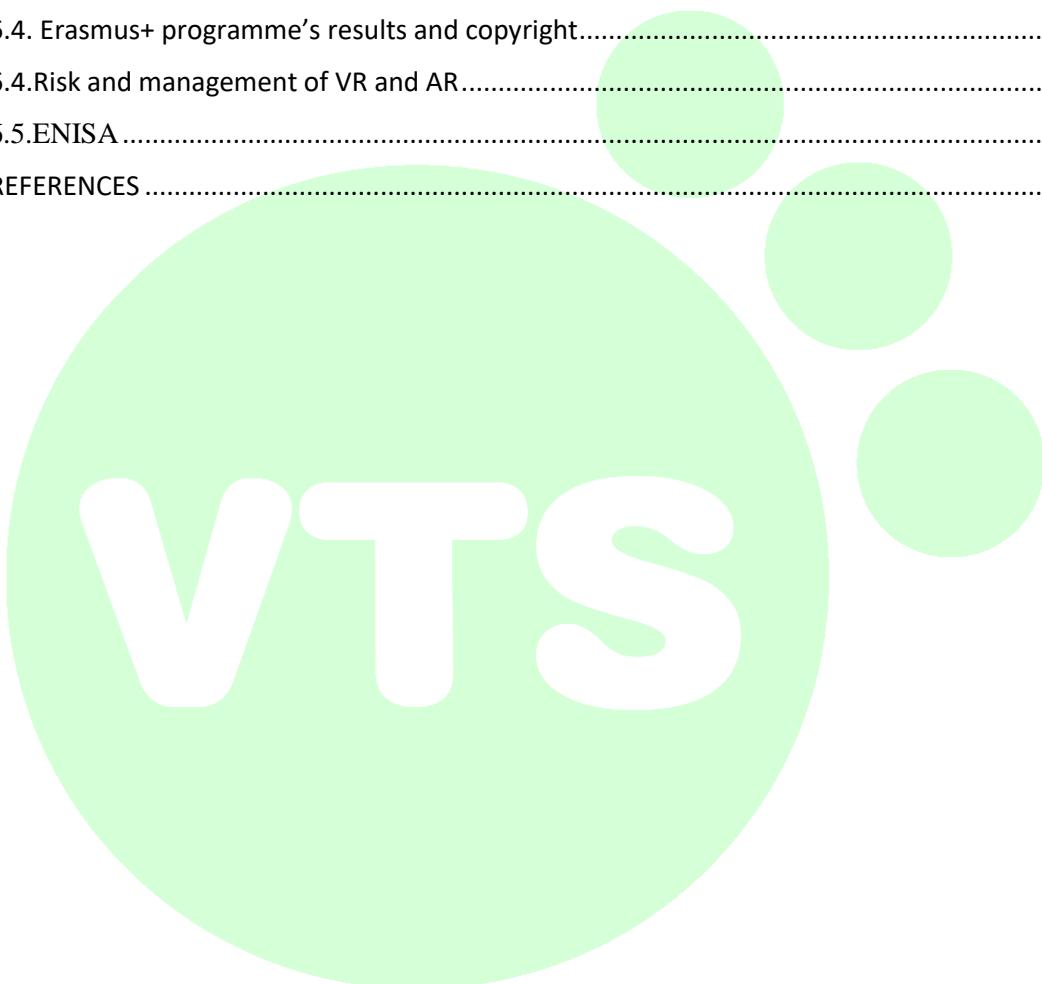
Disclaimer

"Funded by the Erasmus+ Program of the European Union. However, European Commission and Spanish National Agency cannot be held responsible for any use which may be made of the information contained therein".



Contents

CHAPTER 6 – LEGAL SKILLS: LEGAL ORGANIZATION FORM, RISK MANAGEMENT, PRIVACY AND SECURITY	4
6.0 The Legal Aspect.....	4
6.1. The importance of security	4
6.2. Law and Virtual Reality.....	5
6.3. Common Creative.....	6
6.4. Erasmus+ programme's results and copyright.....	7
6.4. Risk and management of VR and AR.....	8
6.5. ENISA	9
REFERENCES	10



CHAPTER 6 – LEGAL SKILLS: LEGAL ORGANIZATION FORM, RISK MANAGEMENT, PRIVACY AND SECURITY

6.0 The Legal Aspect

The legal aspect is extremely important. This also applies to IT-related activities. Each photo, text,. music, film or meme is the result of someone else's work and is protected by copyright. This also applies to computer applications and the audiovisual material used in them.

New technologies are becoming more and more available and common, what is more the development is so fast that it may become a difficult problem for the law to keep pace with the advancements in IT technology. The way of using them has to be adapted to the existing regulations or new regulations should be created which means this is a continuous and endless process. The problem may not only be the use of VR and AR applications and the related copyrights but also the impact of these technologies on human's mind and body which can cause psychological problems and violate someone's privacy.

There is much debate about the potential dangers and threats related to the use of virtual worlds. According to the scientists, there is always a potential risk as no software is 100% safe (Smedinghoff, T). VR and AR can collect many data such as: human movement, sounds from the environment, biometric data (e.g. pupil measurement), location information (e.g. computer IP), device information (type, software, applications). All these data that can be used for various purposes sometimes not legal. The question appears: What should be done to protect the users?

6.1. The importance of security

New technologies are becoming more and more available and common. However, the use of VR and AR is a problem difficult for the law. The way of using them has to be adapted to the existing regulations or new regulations should be created. It is a continuous and



endless process. The problem is not only the use of VR and AR applications and the related copyrights. VR and AR technologies, creating a virtual world, can also cause psychological damage and violate someone's privacy.

There is much debate about the potential dangers and risks of using virtual worlds. As with all software, there is a risk as no software is 100% safe (Smedinghoff, T.). Data that VR and AR can collect are: human movement, environmental sounds, biometric data (e.g. pupil measurement), location information (e.g. computer IP), device information (type, software, applications) (Jerome J., Greenberg J.). Twenty minutes of using VR can generate about two million data, including body language (Bailenson J.,). Protecting this data is a job for IT professionals who need to create security software, and for lawyers who need to legislate for data capture and processing.

6.2. Law and Virtual Reality

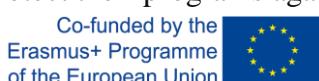
Legal issues related to VR I AR may concern (Virtual legality Virtual Reality and Augmented Reality - Legal Issues): intellectual property, privacy protection, product liability, use in criminal activities. Some scientists even use the term VR/AR street crime (Mark A. Lemley and Eugene Volokh). In their work they conclude that: „VR and AR will present challenging issues for the law. Many such issues will require adapting existing doctrines to new circumstances or modifying legal rules to take account of new facts. We don't have definitive answers to these questions; our purpose in raising them is to begin the process of thinking about them.”

Intellectual property is protected by law, for example if the developer creates an application for an entrepreneur, the contract between them should specify who owns the copyright to the product. Most often, the creator transfers the copyrights to the ordering party.

The lack of such arrangements in the contract makes the issue of intellectual property unclear and may be a source of future disputes. Most often compensation may be demanded for infringement of copyright.

However if VR and AR applications are available on the basis of free copyrights, using them does not threaten legal consequences. That is why the user should always make sure if using the application of its elements is not protected by copyrights.

Most companies are trying to protect their programs against data theft. This is important



especially in the case of corporations. An example is the Oculus company, which protects privacy at the level of goggles. It also uses special anti-theft protection programs (Oculus for Business | Virtual reality for enterprises).

The developer of VR and AR software should provide information about the target group. It should also inform the potential user about the negative effects of using (e.g. contraindications for use - it may be a motion sickness).

Illegal use of VR and AR applications may be punishable. Trading apps without copyright is also a crime. There are also situations where VR can help in detecting perpetrators of crimes. An example is the Kozminski University in Warsaw, where VR has also been used in forensics classes for several years. Thanks to the use of this technology, students have the opportunity to inspect the crime scene (Mikołajczyk).

6.3. Common Creative

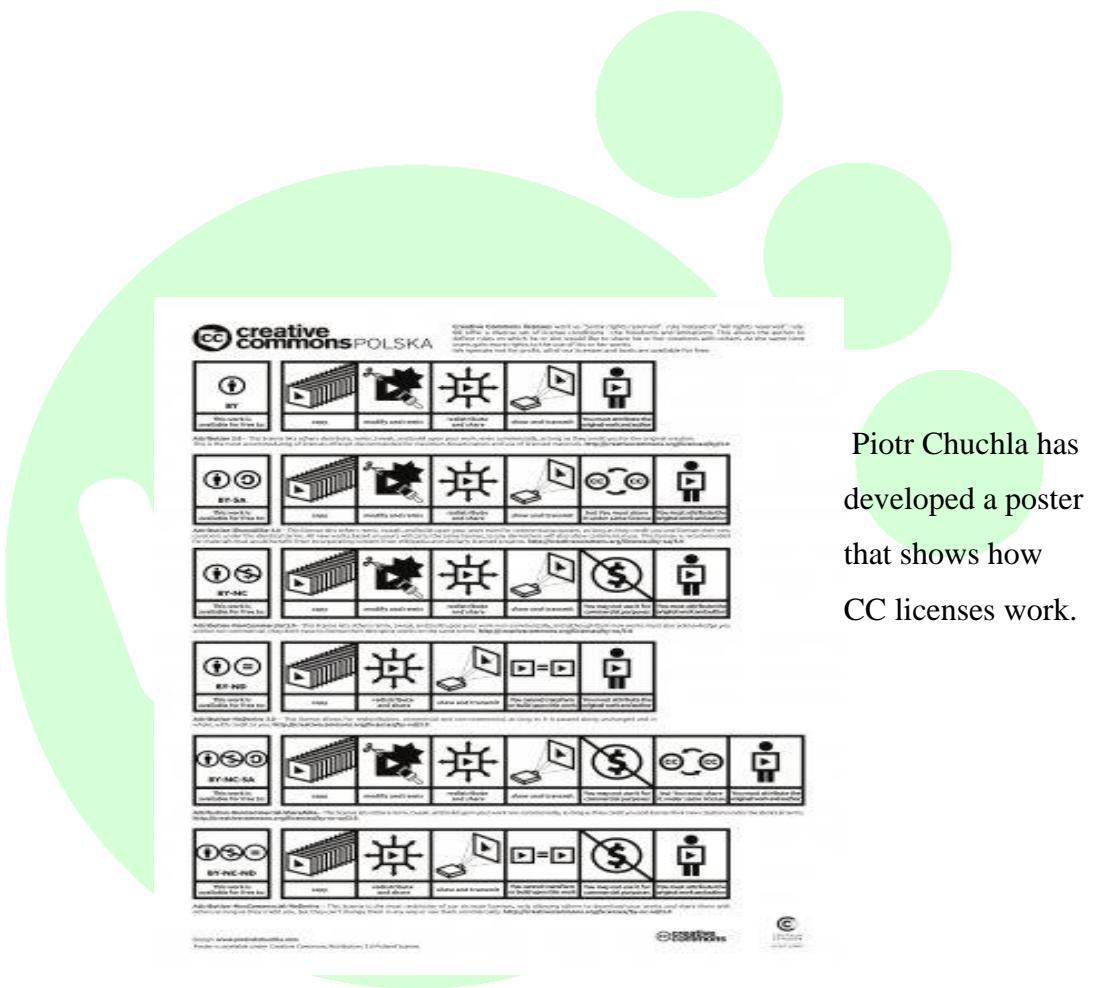
Creative Commons is an international project offering free legal solutions and other tools for authors to manage copyrights to their works. Creative Commons supports free culture: the production and exchange of works treated as the common good. Creative Commons was established in 2001 as an American non-governmental organization, established on the initiative of scientists (mainly lawyers) and intellectuals involved in work for the protection and promotion of common cultural goods. The basic tool of Creative Commons are legal licenses that allow replacing the traditional model of "All rights reserved" with the principle of "Certain rights reserved" - while respecting the principles of copyright. Creative Commons licenses offer a diverse set of licensing conditions - freedoms and limitations. Thanks to this, the author can independently define the rules on which he wants to share his work with others.

The four basic license terms Common Creative

 – Credit must be given to the creator

 – Only noncommercial uses of the work are permitted

- ≡** – No derivatives or adaptations of the work are permitted
- ©** – Adaptations must be shared under the same terms



The picture: The poster of CC (<https://creativecommons.pl/2012/06/plakat-o-licencjach-cc/>)

6.4. Erasmus+ programme's results and copyright

Erasmus + beneficiaries are required to publish the results of their work (documents and materials prepared during project activities) on the Internet under open licenses. In this way, access to valuable materials that are helpful in learning, teaching, training and

working with young people will be broadened. People who want to use works made available under open licenses do not have to individually obtain consent from the author. All results must be obligatory posted on a special platform. This is the platform address:<https://erasmus-plus.ec.europa.eu/projects>

6.4.Risk and management of VR and AR

The use of VR and AR involves various risks. An example is the use of VR resulting in the collection of additional information by the virtual social network VRSN (eye movement, emotions, real-time reactions). This means that more and more user data can be digitized and (potentially) made available to entities who may misuse it. Both application developers and their users should be aware of the risks they pose.

These are some of them (ORGANISING A CYBER CRISIS MANAGEMENT EXERCISE): Intensity and ubiquity of impacts; Potential long-term uncertainty; The capacity to be changed in size or scale; Responsibility of VR and AR technicians; Rate of spread of cyber attacks; Repeatability of cyber attacks; The time it takes to recover from a cyber attack; Difficulties in determining the source of a cyber attack.

Use of VR by children raises a number of specific privacy and ethical issues. It should be monitored as excessive use may be addictive or reduce face to face contact. It should also be mentioned that using VR can cause cyber sickness which is similar to seasickness or motion sickness. The negative effects and malaise may be felt more or less. It depends not only on human condition but also on the type of hardware and software. With better motion simulation devices, we can minimize the risk of experiencing the negative effects of VR disease (Lee Jiwon, Mingyu Kim, Jinmo Kim).

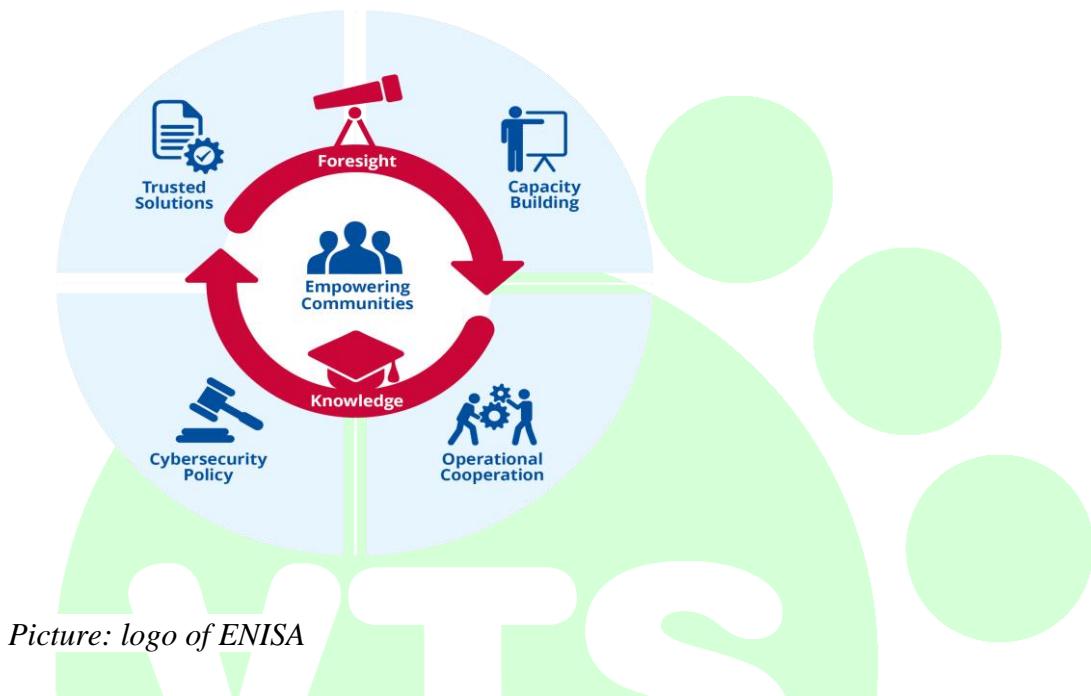
We use technology more and more and we use it more and more. It is not only about searching for information, but also making payments, concluding contracts, etc. This raises problems in terms of data protection and security.

Privacy and security issues can also apply to VR. In many games, players create avatars, equip them with specific features (J. Zimmer-Czekaj), they can be not only external features but also character traits.

There is a need for a definition of virtual property. Virtual property may mean computer code with which objects from the real world are imitated or software code designed to behave and possess the properties of material mobility from the real world or particles of reality or objects and objects occurring in virtual worlds (J.W. Nelson).

6.5.ENISA

The European Union Agency for Cybersecurity, ENISA. This is EU agency. The goals of ENISA are: Empowering Communities, Cybersecurity Police, Operational Cooperation, Capacity Building, Trusted Solutions, Foresight, Exchange Knowledge and Experiences.



ENISA was created in 2004. Its Regulation is the Regulation (EU) 2019/881 of the European Parliament and of the EU Council of 17 April 2019 (Cybersecurity Act) on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

In the structure are: Management Board, Executive Board, Executive Director, National Liaison Officers Network, Advisory Group, Ad hoc Working Groups.





Picture: the poster of the international conferences about safety of cyber world.

ENISA (in cooperation with Danish Health Data Authority) was the organizer of series of virtual eHealth Security conferences in on cybersecurity topics touching the Healthcare sector (Picture). They invited professionals from the healthcare sector and experts in cybersecurity to share their experiences and challenges through open discussion sessions (<https://www.enisa.europa.eu/>).

REFERENCES

<https://www.computerlaw.com/articles/the-law-of-virtual-reality/#2.4>

<https://www.internetlawyer-blog.com/augmented-and-virtual-reality-laws-part-i/>

<https://www.enisa.europa.eu>

New EU Cybersecurity Strategy (europa.eu)

Directive on measures for high common level of cybersecurity across the Union

[Digital Europe Programme](#)

[Commission Recommendation on the Cybersecurity of 5G network](#)

New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, December 2020

ORGANISING A CYBER CRISIS MANAGEMENT EXERCISE, Dépôt légal : septembre 2021 AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Virtual legality Virtual Reality and Augmented Reality – Legal Issues

Bailenson Jeremy, Protecting Nonverbal Data Tracked in Virtual Reality, J172 AMA Pediatr. 905 (2018), available at
<https://jamanetwork.com/journals/jamapediatrics/article-abstract/2694803c>

Jerome J., Greenberg J., AUGMENTED REALITY + VIRTUAL REALITY . Privacy & Autonomy Considerations in Emerging, Immersive Digital Worlds, 2021

Kaczmarczyk B., Szczepański P., Dąbrowska M., Wybrane zagadnienia cyberbezpieczeństwa, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy, 2019.

Karkut Daniel, Własność wirtualna. Problemy definicyjne i perspektywa polskiego prawa, Uniwersytet Wrocławski Wydział Prawa, Administracji i Ekonomii.

Lee Jiwon, Mingyu Kim, Jinmo Kim, A Study on Immersion and VR Sickness in Walking Interaction for Immersive Virtual Reality Applications, 2017.

Lemley A. Mark and Eugene Volokh, LAW, VIRTUAL REALITY, AND AUGMENTED REALITY, April 2018.

Matusiak I., Avatar jako przedmiot tzw. własności wirtualnej: powstanie, korzystanie i obrót – aspekt autorskoprawny, „Wrocławskie Studia Sądowe” 2014.

Mikołajczyk Katarzyna, “VR w edukacji – subiektywny przegląd możliwości”, Warsaw 2019.

Nelson J.W., A Virtual Property Solution: How Privacy Law Can Protect the Citizens of Virtual Worlds, „Oklahoma City University Law Review” 2011, vol. 36.

Smedinghoff, T., Online Law: The SPA’s Legal Guide to Doing Business on the Internet. Thomas J. Smedinghoff, Editor, Reading MA: Addison-Wesley Developers Press 1996.

Wilk Angelika, Katarzyna, Wirtualna rzeczywistość – wsparcie czy zagrożenie dla bezpieczeństwa?, Politechnika Warszawska Wydział Zarządzania, Warszawa 2018

J. Zimmer-Czekaj, Prawa własności intelektualnej w wirtualnych światach, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Właściwości Intelektualnej” 2009.

Barcelona, Spain (2021)

© Copyright VARTES partnership 2020-2022 (grant no. 2020-1-ES01-KA204-082270)

Creative Commons (CC) licence: everyone is welcome to share, use and build upon our work.

"Funded by the Erasmus+ Program of the European Union. However, European Commission and Spanish National Agency cannot be held responsible for any use which may be made of the information contained therein".

