Legal Study on the Radio Equipment Directive’s Potential Ramifications for FOSS

(May 15, 2019)
Legal Study on the Radio Equipment Directive’s Potential Ramifications for FOSS

I. Goal of this study

The goal of this study is to investigate potential ramifications of the Radio Equipment Directive’s (hereinafter referred to as “RED”) legal requirements – notably Art. 3 (3) (i) – for Free and Open Source Software (FOSS) and the many products that rely on it. In particular, this study seeks to evaluate whether or not the inclusion of certain classes of hardware devices into the scope of the directive will lead to incompatibilities with FOSS license terms such as the GNU General Public License, version 3 (GPL-3.0).¹

II. Relevant provisions of the Radio Equipment Directive

The European Parliament passed the Radio Equipment Directive (2014/53/EU) in 2014. The overall goal of the directive is to regulate devices that rely on radio signals² and integrate wireless technologies, for example, laptops, mobile phones, routers and many IoT devices such as smart trackers or kitchen appliances.³ The RED harmonizes existing regulations and provides requirements for economic operators to increase the security of radio spectra as well as safety and security of radio equipment. Member states were required to implement the directive into national law by the middle of June 2016. For example, the relevant German law is the “Gesetz über die Bereitstellung von Funkanlagen auf dem Markt” (Funkanlagengesetz - FuAG) from June 27, 2017.

¹ Hereafter we use the SPDX-Identifiers as abbreviations for FOSS licenses, see https://spdx.org/licenses/.
² See Recital 6: “Equipment which intentionally emits or receives radio waves for the purpose of radio communication or radio determination”.
³ Commission Decision (EU) 2018/637, Recital 2: „The Internet of Things (IoT) generally refers to the interconnection via the internet of devices embedded in everyday objects, which enable these objects to exchange data. Wireless IoT may also be realised through electronic communications services based on cellular technologies, which normally make use of licensed spectrum. Wireless IoT applications serve a wide range of industrial sectors such as energy or automotive and rely on spectrum availability.”
Subsequently, this study will focus on one particularly disputed requirement set forth in Art. 3 (3) (i) of the directive, which obligates device manufacturers to check every software that can be loaded on the device for compliance with applicable radio regulations and to ensure that third parties are not able to install modified versions of such software. This requirement represents a shift of responsibility for compliance of modifications from the users to the manufacturers. To understand the full implications of this norm, it is important to look at several provisions of the RED in more detail.

1. **Scope of the directive**

According to Art. 1 RED the directive applies to “the making available on the market and putting into service in the Union of radio equipment”. Art. 2 RED defines radio equipment as "an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radio determination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radio determination”.

Thus, the RED has an very broad scope since “radio waves” are defined as “electromagnetic waves of frequencies lower than 3 000 GHz, propagated in space without artificial guide” and therefore technologies including micro waves, mobile telephony, television, wifi, Bluetooth, GPS, radar and others are covered under the RED as well.⁴

While there are exceptions for certain types of equipment according to Annex 1 to the RED, for example for equipment exclusively used for activities concerning public security and defense, for radio equipment used by radio

---

amateurs or for custom-built evaluation kits destined for professionals at research facilities, the definition of a radio product under the RED is nevertheless broad enough to generally cover a whole array of consumer products such as routers, cellphones, laptops and smart appliances. It is important to note, though, that according to Art. 2 (2) the Commission may adopt implementing acts to determine whether certain categories of electrical or electronic products meet the definition of a radio product and that according to Art. 3 (3) the Commission may specify which categories or classes of radio equipment Art. 3 (3) (i) applies to. Therefore, there is no final list of hardware that is affected by the directive yet. Currently, an “Expert Group on Reconfigurable Radio Systems” (EG RRS) is working on a proposal for which categories shall fall under the scope of Art 3 (3) (i) and which ones shall not.

2. “Lockdown” requirement of Art. 3 (3) (i) RED

a. Obligation to include technical protection measures

The RED provides a list of requirements that radio equipment needs to meet in Art. 3. The most controversial requirement is set forth in Art. 3 (3) (i) RED. According to this norm, radio equipment within “certain categories or classes” shall be constructed so that it

“supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated”.

The Commission shall be empowered to adopt delegated acts in accordance with Article 44 RED specifying which categories or classes of radio equipment are concerned by this requirement (and other essential requirements listed in Art. 3 (3)). Recital 16 explains the rationale behind this requirement:

---

“The compliance of some categories of radio equipment with the essential requirements set out in this Directive may be affected by the inclusion of software or modification of its existing software. The user, the radio equipment or a third party should only be able to load software into the radio equipment where this does not compromise the subsequent compliance of that radio equipment with the applicable essential requirements. “

b. Shift of legal responsibility from the user to the manufacturer

This obligation is primarily addressed to the manufacturer (Art. 10 RED), who needs to ensure that radio equipment that is put on the market will be built in a way that technically prevents non-compliant software from being loaded onto a hardware product. Manufacturers can achieve this result by employing technologies like cryptographic signature checks (e.g. secure boot which can secure the boot process by preventing the loading of drivers or loaders of the operating system that are not signed with a specific digital signature), which ensure that only software with a valid signature can be installed. Thus, the free access of the user to the Radio Equipment to allow him or her to install modified software has to be suppressed.

Before this norm came into effect, manufacturers of certain security-sensitive products such as cars or medical equipment already used such technological protection measures in order to prevent users from changing the software of the product. However, the norm represents a shift in terms of legal responsibility. Security-sensitive products often require a permission or registration of some sort. Until now, once the user tinkered with the software, he or she would lose said registration and would be legally responsible for potential damages that resulted from these modifications and/or the user would be not allowed to publicly use such devices.⁶ The RED now places

---

⁶ As an example, see sec. 19 para 2 and 3 of the German Road Traffic Licensing Regulations (StVZO). The vehicle’s permission to operate ceases if modifications are made which are likely to endanger road users.
the legal responsibility on the economic operators (i.e. notably manufacturers (Art. 10), and to some degree on importers (Art. 12, 14) and distributors (Art. 13, 14)). They must ensure that it is technically impossible for users or third parties to change the software where the combination of the radio equipment and software has not been demonstrated to be compliant with the RED.

c. Penalties for failure to comply with Art. 3 requirements

Pursuant to Art. 46 RED, member states shall lay down rules on penalties applicable to infringements by economic operators. In Germany, for example, the requirements of the RED were transposed into national law by the Gesetz über die Bereitstellung von Funkanlagen auf dem Markt (FuAG). The requirement of Art. (3) (3) (i) RED is transposed in § 4 (3) No. 9 FuAG. § 9 (1) FuAG then stipulates the responsibility of the manufacturer for building radio equipment pursuant to the requirements mentioned above, i.e. in practice including the obligation to include technical protection measures. § 37 FuAG provides for a penalty of up to 100,000 Euro should the manufacturer fail to comply with § 9 (1) FuAG.

d. Commission to determine classes of products covered by Art. 3 requirements

It is important to note that the legal text does not name the classes of products that need to be built in accordance with the requirements of Art. 3 (3) (i), but leaves it to the Commission to adopt delegated acts that specify these classes (Art. 3 (3), paragraph 2 and Art. 44 RED). The Commission is expected

7 „Funkanlagen bestimmter Kategorien oder Klassen müssen, sofern und soweit die Kommission gemäß Artikel 44 der Richtlinie 2014/53/EU dies in delegierten Rechtsakten festgelegt hat, so gebaut sein, dass sie die folgenden grundlegenden Anforderungen erfüllen: … 9. Sie unterstützen bestimmte Funktionen, mit denen sichergestellt werden soll, dass nur solche Software geladen werden kann, für die die Konformität ihrer Kombination mit der Funkanlage nachgewiesen wurde.“
to finish and publish said delegated act no earlier than at Q1 of 2020.\textsuperscript{8} It currently appears likely that the Commission will include many IoT devices, routers, cell phones etc. that rely heavily on FOSS in classes of products that need to be built in accordance with Art. 3 RED.\textsuperscript{9}

III. Potential conflict with FOSS license terms

As explained above, Art. 3 (3) (i) RED essentially requires radio equipment manufacturers to implement technical protection measures that prevent users (or other third parties) from installing software where the compliance of the combination of the radio equipment and software has not been demonstrated. This may not only conflict with the idea of Free Software,\textsuperscript{10} but also with the license terms of specific FOSS licenses.

To illustrate the conflict this may create with FOSS, it is necessary to take a closer look at the license conditions of the GNU General Public License, versions 2.0 and 3.0.\textsuperscript{11} These are licenses with a strict Copyleft policy (i.e. licenses using copyright to ensure that all modifications of a program must be licensed under the original license free to everyone)\textsuperscript{12}. Some of the most important Free Software, such as essential components of the GNU/Linux operating system are licensed under the GPL-2.0. Linux is widely used in IoT, routers and many other devices using Wi-Fi or other radio waves for communication.

The Free Software Foundation published version 3 of the GNU General Public License in 2007. This license has also gained a relevant market share. To give a practical example: Samba is a Free Software re-implementation of the


\textsuperscript{10} See https://www.gnu.org/philosophy/free-sw.html.

\textsuperscript{11} Equivalent terms are within LGPL-3.0 and AGPL-3.0.

\textsuperscript{12} https://www.gnu.org/copyleft/.
SMB networking protocol under GPL-3.0 and used in many routers and other devices.

1. “Installation Information” and GPL-3.0

Section 6 of the GNU GPL-3.0 addresses the issue of technical protection measures directly. It requires manufacturers of products that are “User Products” and that use GPL-software to provide the “Installation Information”. To give some background to this requirement, the so-called “Tivoization” problem was a concern when the license text of the GPL-3.0 was drafted.\(^\text{13}\) TiVo, a manufacturer of hard-drive recorders, used a Linux system, whereby the re-installation of modified software was made impossible by a digital signature check. The Free Software Foundation opposed this as a restriction of user freedom and included a license clause in the new version 3 of the GPL, according to which the user must be provided with the appropriate means so that new program versions can also be installed when such DRM technology is used:

> “Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

> If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of

\(^\text{13}\) See https://www.gnu.org/licenses/gpl-faq.html#Tivoization.
how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information.”

However, this obligation is restricted to so-called “User Products”. A “User Product” is either a consumer product, which means any tangible personal property which is normally used for personal, family, or household purposes, or anything designed or sold for incorporation into a dwelling.\textsuperscript{14} Many of the products potentially covered by the RED such as routers or smart household appliances are “User Products”. Providing “Installation Information” means that the manufacturer has to enable the user to change the software and to load it back on. Therefore, at least where User Products are concerned, the obligation in Art. 3 (3) (i) RED, “to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated” and the license conditions of the GPL-3.0, AGPL-3.0 and LGPL-3.0 are incompatible.

It should be noted that the violation of license conditions of the GPL-3.0 results in an automatic termination of rights.\textsuperscript{15}

2. “Scripts to control installation” and GPL-2.0

The GPL-2.0 does not contain any explicit provision on DRM techniques. As a result, the FSF obviously considered this to be an unclear legal situation or even permissible and therefore decided to solve the problem in a new license version (see above). But this does not mean inherently that the use of digital signatures or the like is allowed without restrictions under GPL-2.0. In contrary, section 3 GPL-2.0 shows that the user should be able to reinstall modified programs when defining the term “complete corresponding source”:

\textsuperscript{14} See the definition of the Magnuson-Moss Warranty Act, https://www.law.cornell.edu/us-code/text/15/2301.

\textsuperscript{15} See sec. 8 GPL-3.0.
“For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable.”

At least under the application of German contract law, the GPL-2.0 can be interpreted as meaning that although technological measures to control the installation are permissible, the user must nevertheless be able to install modified versions of GPL-software. This is underlined by the fact that the GPL-2.0 is intended to give users the freedom to modify the software, as is made clear in the preamble:

„Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs.”

This seems to be just as much a conflict with the requirements of Art. 3 (3) (i) RED as it is with the GPL-3.0.

3. “Relink to produce a modified library” and LGPL-2.1

The GNU Lesser General Public License, Version 2.1 (LGPL-2.1) is a license for program libraries with a “weak Copyleft”, i.e. not all derivative works need to be licensed as Free Software under the LGPL-2.1 rather only modifications of the library itself. Applications linked with the library may be distributed under proprietary license terms or other FOSS licenses. Nevertheless, the LGPL-2.1 has specific requirements for the distribution of applications linked with the LGPL-library.

In particular, the LGPL-2.1 requires in its sec. 6 that the user must be enabled to relink modified software libraries under the LGPL with applications that are distributed linked with the LGPL-2.1-libraries:

“…so that the user can modify the Library and then relink to produce a modified executable containing the modified Library.”

“Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user’s computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.”

This is a very common situation since most Linux based products use a standard C library under the LGPL-2.1 (e.g. GNU C Library) and nearly all applications running on Linux need to be linked with such a C library. 17

IV. Summary

As far as the most important Free Software licenses are concerned, i.e. the GNU General Public License and the GNU Library General Public License, the license conditions of said licenses are in contradiction to of Art. 3 (3) (i) RED which requires it to be ensured that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated. This is particularly true for all software under GPL-3.0, LGPL-3.0 and AGPL-3.0 but is very probable to be relevant for GPL-2.0 and LGPL-2.1-licensed software as well.

17 https://www.gnu.org/software/libc/.
Art. 3 (3) (i) RED applies only to such classes of products that are specified by the Commission in delegated acts according to Art. 3 (3), paragraph 2 and Art. 44 RED. Delegated acts have not yet been adopted. Therefore, the economic impact of the RED remains unclear.

It can be stated that widely used Free and Open Source Software programs as GNU/Linux, GNU C Library and Samba will not be able to be used in products which fall into the scope of Art. 3 (3) (i) RED if the delegated acts of the European Commission do not provide for a limitation. Otherwise, the manufacturer would risk a copyright infringement since any violation of the license conditions of the GPL and LGPL results in an automatic termination of the rights granted.

Berlin, 15.05.2019

Dr. Till Jaeger
Attorney-at-law