



FIcontent



DEVELOPING APPLICATIONS FOR SOCIAL CONNECTED TV

GUIDELINES FOR DEVELOPERS AND CONTENT PRODUCERS



Developing applications for Social Connected TV

Guidelines for developers and content producers

Editor: Martin Gordon / Rundfunk Berlin-Brandenburg

Design: Andreas Perzborn / buero-perzborn.com



Contents

Part 1: Social Media Guidelines	7
Introduction	7
Broadcasters and social media engagement.....	9
Impact on journalists	9
Broadcasters' behavioural guidelines.....	10
Branding	11
Content design for social networks.....	11
User communication and monitoring.....	11
Legal issues.....	12
Developers/content producers and social media engagement	12
Copyright	12
Privacy policy	13
Use of Facebook social plugins	13
Engagement with users.....	14
Part 2: Usability Guidelines	15
Introduction	15
Content display.....	16
Navigation	17
Remote control buttons	17
Coloured buttons	17
Full/minimised view	18
Focus.....	18
Back navigation	19
Universal settings.....	19
Assigning control functions.....	20
Cross-application navigation	20
Display of date and time	21
Feedback.....	21
Accessibility	21
Design.....	22
Personalization for accessibility	22
Options	23
Best Practice example.....	23



Content quality 23

Design of apps for the second screen..... 24

Control using second device 24

Second device connection status 25

Remote control of the application..... 25

General quality standards - switching applications..... 25

Launching apps..... 26

Return to manufacturer portal 26

Part 3: Data & Privacy 27

Introduction 27

Background..... 27

ARD Data Protection position paper 28

Personal data 30

Sensitive Personal Data..... 30

Collection of and access to Personal Data 30

Sharing Personal Data..... 31

Personal Data for other projects or marketing 31

Privacy notice..... 32

Third party data handling..... 32

Use of online tracking tools 32

Anonymisation 33

Data storage management by users..... 34

Collecting and accessing personal data 34

Data Collection policy 35

Opt-out 35

Right of user access to data 35

Content producer data protection and security..... 35

Policies & personnel..... 36

Recommended practices for security of personal data 36

Resources..... 38



The FIcontent project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. FP7-603662-FI-CONTENT 2.

This document reflects the author/s views and the EU Commission is not responsible for any use that may be made of the information it contains.



FIcontent project site:

<http://mediafi-org>



<http://europa.eu/>

SOCIAL MEDIA GUIDELINES



Introduction

These Social Media Guidelines are based upon broadcaster recommendations for media producers/editors producing content for own platforms, for third-party platforms and for self-operated social media platforms.

What do we mean by 'social media'? The term is broad; it can refer to social networks (such as Facebook), blogs (such as Wordpress), social bookmarking services (Digg), microblogging services (Twitter) or to other interactive platforms such as YouTube, Flickr and Instagram. All these services revolve around user participation.

The development of social networks and other interactive platforms is still in a formative stage. The number of social media users, especially younger users, increases daily; many young users source their complete information input from social media, as well as a significant portion of their social interaction. Even content which is not directly part of social media or interactive platforms, such





as editorial content produced by professional broadcasters and publishers, is often incorporated into the social media environment; smartphones and other mobile devices are leading to an increasingly mobile use of social media offers. Social networks are also increasingly used by companies for promotional purposes, and play an expanding role for media editors as research and feedback tools.

The editorial work of broadcasters reflects the reality that social networks have become important communications channels. Social media users and the related platforms perform the various roles of producer, commentator, gatherer, joiner and observer. Social media users provide comment and feedback, they document and observe activity, and they deliver information and participate in activities flagged up by social media. Broadcasters now increasingly acknowledge the activities of these users by integrating social media into their daily workflows.

Broadcasters increasingly allocate effort to analysis of various feedback and social media channels, which provide editors with topics and content. Thus broadcasters' online strategies are of relevance to users of social media and to content producers who seek to use social media to enhance the visibility of their content:

- developers creating applications for broadcast use should be aware of the increasing impact of social media on broadcasters, and of the implications and restrictions resulting from the expanding role of social interaction in media;
- content producers should be aware of the role of social media within broadcasters, and within the broadcast environment into which social media is incorporated.



Broadcasters and social media engagement

Broadcasters have responded to the development of social media in various ways:

- some broadcasters operate their own social networks;
- some broadcasters broadcast their own content via existing social networks;
- editorial procedures of broadcasters journalists and newsroom structures are adapted as social media activity is incorporated in broadcast output;
- groups of users disseminate broadcasters' content via their own networks.

Establishing a social media presence often requires very little effort in terms of operation, maintenance and technical development, and offers the possibility of quickly-implemented action. This is attractive for a broadcaster; however the quantity of social media outlets makes it necessary for broadcasters to develop meaningful know-how in order to benefit from the possibilities offered by these outlets.

Impact on journalists

Close contact with users of social networks increasingly impacts journalistic work, as when social network users are recruited as eyewitnesses to events or as interviewees. The previously one-way transaction between media companies and viewers/users is replaced by an interactive and ongoing exchange between the journalist and the consumer of the information. Users of social media also affect the perceived priority of various issues, topics and stories and, by their activity, can generate or focus attention upon new topics of interest.

For broadcasters and other content producers, successful engagement in social networks requires additional editorial effort. These formats produce communications which require monitoring and supervised by the broadcaster. Broadcasters must also respond to users; faced with a lack of support and response, users turn away. Where broadcasters are involved with a variety of social media platforms, there is a risk of fragmentation. In the worst case, this can cause the broadcaster to neglect the development of its own online formats.

Risks for broadcasters

The participation of broadcasters in social media platforms can be seen as an official seal of approval. Any breakdown in communication between broadcaster and social platform user may be attributed to the broadcaster. Depending on the type of presence in the social networks, the broadcaster may lose control of its content or its brand representation. Misconduct in social networks, such as failure to observe data protection issues, may have a negative effect on the broadcaster. Employees also communicate privately in social networks, and the separation of personal and professional actions is often difficult; misconduct in the private sector may negatively impact the broadcaster. Thus broadcasters require their employees to follow strict codes of conduct. Broadcasters' behavioural guidelines.

Broadcasters have guidelines for staff behaviour online which determine their possible actions and interactions. Typical broadcaster policy requires that:

- editors/content producers act professionally in observing broadcaster corporate policy as well as legal requirements when interacting with users via social networks and platforms;
- all postings, blogs, tweets and other posts by journalists are subject to the same rules and standards as other journalistic activities;
- postings, blogs, tweets and other require care and attention, including regular monitoring of user-generated content (UGC);
- UGC is in general published only after prior approval by the relevant editor;
- broadcasters recommend that journalists answer user questions directly whenever possible. For standard questions, FAQs can be used;
- the tone of any communications should reflect the 'official' tone of the relevant programmes/channels as well as that of the platform target group. Communication should be open, friendly and respectful;
- criticism of the broadcaster which is not offensive should be tolerated. If any response to criticism is necessary, journalists are usually expected to consult program area management before responding in a timely and 'open' manner;
- if user contributions are offensive, the user should initially be warned, before subsequent sanctions (suspension, exclusion) are brought into effect.



Branding

As noted, broadcasters' engagement with social networks can be perceived as 'official', authorised participation. Social media helps to develop and strengthen the connection between broadcaster and existing users, and to attract new users. For this reason, broadcasters will include an obvious link to their own platforms in social media activity.

Public service broadcasters will generally provide access to external content at no additional cost to users, where possible in an ad-free environment and without barriers to access. Broadcasters ensure that a clear distance from third-party content or comments is maintained.

Content design for social networks

Content presented via social networks serves as dissemination of broadcaster content, events and activities, in addition to heightening interaction with viewers/users of specific programmes. Thus all posts, blogs, tweets and similar created by broadcasters are subject to the same rules and standards as their other journalistic products.

The general rule observed by broadcasters is that exclusive broadcast content in social networks is not allowed. Content published in networks and on third platforms must always be available on broadcasters' home portals.

Most social networks provide the ability to set up a vanity URL. These URLs are subject to strict brand management just like any other broadcaster-related product.

The design of the profile page (background images, graphics, Facebook App) is part of the regular design workflow of a broadcaster. Most broadcasters will develop templates for use across all internet profiles.

User communication and monitoring

User interaction offers the broadcaster the opportunity to interact with users in real-time, and users also expect this interaction. Thus profile pages require regular care, attention and updating.

For legal reasons, UGC contributions from users will be regularly monitored by supervising editors, usually within 24 hours of the upload of such content. For contentious issues, broadcasters will usually decide in advance of publication whether UGC must be approved in advance or closely monitored, if prior inspection is not possible.



Legal issues

A broadcaster's involvement in third-party social networks may limit its habitual control over issues of data, privacy and the protection of minors. Mutual promotion and linking of third party platforms is subject to applicable press, broadcasting, data protection and copyright law.

Developers/content producers and social media engagement

Broadcasters apply consistent journalistic standards to all forms of content. Contributors should ensure that content observes broadcast standards, including:

- accordance to general laws, laws protecting minors and individual rights;
- maintenance of objectivity and impartiality of reporting, diversity of opinion and balance;
- review of statements of fact;
- indication of conjecture;
- ensuring that the subjects of any coverage are heard and their opinion is taken into account when creating stories;
- ensuring that interviews or observations are not altered or distorted;
- ensuring that messages and comments are separated from reports - opinions must be recognizable as such;
- ensuring photos and videos are disseminated only with the consent of the rights owner;
- ensuring that images correspond with text and vice versa.
- broadcasters also observe journalistic diligence when linking to external sites; broadcasters continually review external sites for violations of criminal or child protection legislation or any copyright or moral rights violations. Linking to such sites can be a violation of law.

Copyright

Broadcasters usually have no rights to publish agency reports and material hosted by third-party platforms. Before such copyright-protected content is published, broadcasters will ensure that such use is permitted. If this is not the case, rights may be purchased separately. Violation of copyright can be punishable by law.



Privacy policy

Data protection law applies to social media content - users' personal data (email addresses or other personal information provided by users) is likely to be recorded by the hosting platform. Other details may also be recorded, including time of visit, date, IP address etc.

Proprietors of social networks which comply with data protection-requirements will therefore:

- recognize the applicability of the EC Data Protection Directive to the processing of personal data to, even if users are based outside the European Economic Area;
- inform users and users of their identity and provide comprehensive and clear information about their objectives, as well as the various ways in which they want to process personal data sources;
- engage in promotional activities in accordance with the relevant provisions of the EC Data Protection Directive and the EC Directive on privacy and electronic communications;
- offer privacy-friendly default settings, providing users with information and appropriate warnings on potential risks to privacy by uploading of personal data to the social network profile;
- delete discontinued user profiles;
- specify how long data on inactive users is retained;
- pay particular attention to the protection of minors. Users should be allowed in general to adopt a pseudonym.

Use of Facebook social plugins

Facebook allows other website owners to incorporate Facebook functionalities on their own sites as social media plug-ins, providing Facebook with information about the pages visited by users. The more sites/pages use these social plugins, the more comprehensively Facebook can capture the surfing behaviour of its users.

This can violate provision of applicable data protection and privacy law - public service broadcasters in Germany avoid use of such social plug-ins as far as is possible. If such avoidance is impossible, the broadcaster/content provider's privacy policy should indicate that such plug-ins are being used.

Engagement with users

Content producers hosting their own content, whether third parties or broadcasters, know that regular page maintenance and speedy responses are vital to maintain user engagement; faced with a lack of support and communication, users will turn away. This in turn creates more editorial work for the content producer, which has to be monitored and supervised.



USABILITY GUIDELINES



Introduction

These usability guidelines are aimed at developers, designers, content/media producers and distributors working within the TV/broadcast/content creation and distribution domains. The guidelines are intended to support the optimal development and operation of HbbTV, IPTV, Smart TV and Red Button technologies and related applications.

The media-friendly preparation and presentation of content, an intuitive and comprehensible user interface and the harmonisation of operational concepts contribute significantly to the success and acceptance of Connected TV services, and enhance the user's engagement with this technology. To support this engagement, this guide clarifies technical, design and editorial aspects within applications, when switching between applications and in a portal context.

These guidelines aim to optimise quality and to ensure cross-functionality of existing applications. They represent a synthesis of current thinking, and

draw particularly on current requirements in the German market. They are based upon current practices and on user studies carried out by the EU-funded Flcontent project.

In contrast to the proprietary systems of the Smart TV manufacturers, Hybrid Broadcast Broadband TV (HbbTV) is a pan-European standard. HbbTV services supplement hybrid broadband television by delivering additional content. The HbbTV service is launched via the red button (the 'Red Button') on the TV's remote control. This scenario introduces user expectations which differ from conventional web use, and which application development/developers should take into account. The attractiveness of the delivery of this content, tailored to the particular medium, and a consistent user experience, plays a significant role in the success of HbbTV services. Preparation and presentation of content, the design of the user interface and ease of use are all decisive in the creation of an optimal user experience.

In addition to the presentation of HbbTV functionalities via Red Button, it's also possible to access many of these functionalities via the Smart TV itself, operating in 'portal' mode. It is important to ensure that apps function as expected in this portal mode, which is described in detail below.

Content display

Keep navigation paths short and comprehensible - they should be intuitive and easy to learn. It should be immediately clear to a user where he/she is and which functions have been selected. There should be clear feedback given in response to every user action. Columns are particularly suitable for applications with a great navigational depth (i.e. with many levels of hierarchy).

Important aspects to keep in mind:

- the fact that, for HbbTV services, the user is sitting in front of a TV screen;
- the size of the screen. Modern Smart TVs have a relatively large screen and viewers sit at a distance of between two and four meters. This is relevant when making decisions about font sizes, colours, contrast, transparencies and images;
- the amount and location of the information shown. Structure text clearly to increase readability, and avoid long passages of text.



Navigation

Users have expectations and experience gained in other environments (computers, touch screens, gaming etc.), and this should be taken into account in the design of user interface. However, not all users are familiar with on-screen navigation concepts.

In general, all recurring navigation elements, functions and service concepts should be harmonised across apps and functionalities, so that lessons learned in navigation can be universally applied to related services.

Use of the remote control for on-screen navigation is still the main navigation method used by Connected TV viewers. This gives rise to special requirements when designing user interfaces for Connected TV applications.

Remote control buttons

Connected TV users navigate with the TV's remote control. The following buttons are available on the remote control for use in navigation commands:

- arrow buttons
- 'OK' button
- colour buttons
- numeric buttons

The HbbTV standard also allows use of the 'back' button on the remote control. However this button, variously referred to as the 'back', 'return' or 'exit' button is not consistently implemented by TV manufacturers. Use of the 'back' button should be considered as an additional option to the app's integrated 'back' functionality.

Coloured buttons

The remote controller's coloured buttons are generally used for cross-application navigation within services. The labels of the coloured buttons indicate their functions and the linked applications to which they provide access.

The sequence of the colour buttons (red, green, yellow, blue) should not be changed, as it corresponds to the physical arrangement of the buttons on the remote control. The arrangement and labelling of the coloured buttons should remain consistent in order for broadcaster-specific services to be correctly accessed.

Unallocated colour buttons within each application can be used to display content or to provide a function. The buttons should be in solid colours and preferably unlabelled.

Full/minimised view

In full-screen view, all colour buttons should always be displayed. In a minimised view, and on sub-pages, all the functions of the colour buttons should still nonetheless remain accessible.

Numeric buttons

Numeric buttons allow a fast and direct route to often-visited locations but should be used sparingly. When used as navigation aids, they should be primarily offered as cross-application buttons and/or to access often-visited content. The number buttons should always perform comparable functions within similar applications or scenarios.

The '0' button is a cross-application navigation element, and leads to the launch bar within the selected channel. This button should be visible within all applications and sited in close proximity to (and ideally to the left of) the colour buttons.

Focus

Whereas navigation with mouse and touch-screen allows spontaneous access to active navigation elements, the remote control does not allow such spontaneity. Therefore a 'first focus' display is essential, clearly showing which navigation element is currently active.

The focus can be switched between various elements using the remote control. It should always be made clear which element is currently active, which function will be activated or which area will be navigated to. The use should be able to identify the current position of the cursor at all times.

Options for the visual display of the active ('focused') content are:

- display of the border of the active element using a frame outline
- inverted depiction of characters, symbols and graphics within the active content
- coloured differentiation of the active regions / buttons



Back navigation

HbbTV apps should indicate clearly how to return to a previously-viewed page. This is especially necessary in hierarchical menus or when the main navigation menus are not visible in sub-pages:

- the 'back' option must be available at all navigation levels;
- the navigational structures should be as complex as necessary but as clear and simple as possible, using as few menu items as possible;
- graphics should be simple and easily understandable.

Universal settings

Settings which are useful for various applications should be set universally and applied to all services. See also the section on accessibility.

Representation and function of video player controls

The video player is the most critical interface of the various HbbTV implementations of the device manufacturers. The controls of the player should be standardised and arranged identically across all applications. The arrangement, appearance and behaviour of the controls should correspond to currently-existing norms. The appearance of the player bar should also be standardised. It should also be possible to use the remote control's media buttons to control the player.

A minimum set of features should consist of the following controls:

- play / pause
- rewind/forward
- stop
- current position and duration of the video
- full screen / minimise

The following functions are desirable:

- quality settings
- subtitles
- bookmark

There should be a consistent graphic look and layout of video player controls:

-  play / pause – triangle / two parallel dashes
-  stop – square
-  rewind left - left double arrow
-  forward - double right arrow
-  quality settings – gear symbol
-  Subtitles – CC
-  bookmark - '+' – symbol
-  full screen / minimise screen - square with arrow in corner

Assigning control functions:

The following functions should be assigned to buttons:

-  bookmark - adds the video to wish list
-  rewind - rewinds the video
-  play/pause – on click, play symbol changes to pause, pause symbol changes to play
-  stop – stops play
-  forward – advances the video
-  subtitles - subtitles show/hide
-  quality settings - select picture quality of the video
-  full screen/minimize screen - in full-screen mode, the 'minimize full screen' icon is displayed, and vice-versa

Cross-application navigation

If you are providing cross-application navigation, enabling a user to access content from one media library via another media library, navigation should be transparent to the user and should provide the functionality that a user expects. The app should search for the content or service and update coloured buttons accordingly.



Help

Each application should always have a Help function accessible. The Help should ideally be context-sensitive and should explain all current navigation elements.

Label the Help function identically across various applications. The use of numeric buttons for Help excludes functionalities in some contexts, such as when using teletext where numeric buttons call up particular pages.

Display of date and time

All apps should if possible show the current date and time. Depending upon the available space, the following conventions for showing date and time are often used in Germany:

- the date should be always shown and should be separated by full stops – i.e. 01.01.15;
- for the current decade, the date can be shown with 2 numbers; for pre-2010, the year should be shown with four digits;
- displays showing the time should be separated by a colon – i.e. 10:30;
- leading zeros should be used both in date and time – i.e. not 9.30 but 09.30; not 1.1.15 but 01.01.15.

Feedback

Whenever a user has to wait for an action to be completed (i.e. when loading a video), he/she should be provided with visual feedback.

Accessibility

Developers should use all existing technological possibilities to enhance accessibility in Connected TV applications and related apps. When developing new apps, accessibility is as important as usability and attractive design.

The long-term goal of (German public broadcaster) ARD is that all user-programmable options should be selected and stored centrally via a settings app.

- All personalisation options should be easy to find and use;
- Preferences can be stored using cookies if this is technically possible and if agreed by the user;

- It should be possible for users to personalise existing apps for accessibility purposes, or to use the Connected TV to activate additional accessibility functionalities which can be personalised.

Design

Concept developers, graphic designers and web designers should always keep those with accessibility needs in mind; when in doubt, opt for the less ambitious but more usable solution. This applies not only to accessibility issues, but also to general usability issues.

During app development, always consider the following pointers:

- don't use fonts smaller than 18 pixels
- don't use serif fonts
- ensure high contrast of control elements, with no colour gradient and no transparencies
- provide acoustic or visual feedback
- be aware that screen-readers will be used
- content should be tab-navigable

Personalization for accessibility

When designing and implementing Connected TV apps, remember that HbbTV offers the possibility of adapting colour, font size and contrast in order to improve access. Personalisation allows the target group to access other services such as sub-titles. In the case of the ARD, implementation of these options is via stylesheets/CSS.

Use all existing technical capabilities to make the operation of the application accessible to those with disabilities. When designing new apps, give as much importance to accessibility as to attractive design and general usability.

Make it possible for users to personalise existing apps for accessibility purposes or to use HbbTV to activate additional accessibility functionalities which can be personalised.

All options for customization of accessibility should be quickly and easily accessible for HbbTV-users and users. Selected options should be stored via cookies.



Options

If possible, accessibility options should be centrally accessed and presented under a single menu-heading, for example on a 'Settings' page. Viewers should also be able to change accessibility options within individual applications.

The use of a central settings app can enable viewers to simultaneously configure various settings including:

- text appearance and location
- optional sign language interpreter (if sign language translation exists) for live programmes
- audio description for secondary devices (i.e. headphones)
- subtitles for media library
- sign language interpreter for media library
- audio description
- foreign languages/original soundtrack

Best Practice example

The (German public broadcasting network) ARD Text (teletext) functionality is a good example of a best practice implementation of accessibility.

Under the menu 'Settings', users can select their preferred font size and colour options. These personalised settings are stored in a cookie and so are available for the user's next visit to the app.

Viewers can also resize, position and dynamically organise subtitles for the currently-broadcast programme.

The HbbTV users are offered a selection of font sizes and eight colour options for text/background, catering for various degrees of sight impairment. User tests conducted by the ARD showed that the following text/background colour combinations were all requested by testers:

white on blue	blue on yellow	white on red	green on black
black on white	yellow on black	yellow on blue	white on black

Content quality

- all content should be presented and implemented in a user-friendly manner
 - text should be legible;



- use suitable font sizes, create well-structured content and avoid overly long text;
- content provided should be current and regularly updated;
- no blank pages or areas should be shown;
- temporarily unavailable content (i.e. live streams or ticker) should be marked accordingly;
- the current date and time should be shown;
- playable media content should be clearly marked;
- content should not start to play automatically;
- the preferable loading time, either within an app or following a user request, should be a maximum of four seconds;
- provide visual feedback during loading operations.

Where relevant, keep a visual connection with the current broadcast. Options include:

- the scaling of the TV picture to allow both TV broadcast and application to be visible;
- the application is shown as an overlay on the TV screen;
- the application is shown as in a transparent region of the TV screen.

Design of apps for the second screen

The same principles of design of web pages for mobile devices apply to the presentation of the app on the second screen device. In particular, the application should be able to adapt to the particular device and should fulfil accessibility requirements.

Control using second device

HbbTV broadcasts allow for the presentation of accompanying material on a second screen. When users activate a second screen device, their experience in controlling an application via the device should be consistent. User guides and information text should be harmonized – i.e. functions available via the second device (e.g. as 'hide application on the TV') should be described and graphically represented as on the main screen. The activation of the second-screen functionality should be indicated via a recognisable icon.



Second device connection status

The connection status of a device should be shown with a single icon. Possible status can be:

- 'active' (message exchange possible);
- 'inactive' (message exchange not available);
- the application should check the status of the connection continuously and update the display accordingly;
- the connection status should be shown by both devices (TV and second screen device) using the same connection status icon for each;
- the status icon should be positioned at the top of the app to ensure visibility on the second screen device. This is particularly important for mobile devices with touch screens.

Remote control of the application

Control of the app should be possible using the remote controller even after connecting to a second device.

General quality standards - switching applications

If a user switches apps via the second screen device, the devices should remain connected. The newly-selected app should load both on the TV and on the second device. Connection should follow without further intervention by the user.

- direct links between different applications should be offered whenever possible (e.g. as a shortcut);
- when using colour buttons, avoid inconsistent use of the buttons within one channel;
- if two applications already offer content connections, direct links should be set (e.g. program preview and VoD offers);
- colour buttons should be used for switching between core applications;
- use a consistent key allocation across all channels;
- as an alternative to navigating with colour buttons, use links in the form of menu items;
- when using numerical buttons, remember that these may not be available or available only in inconvenient ways, e.g. on devices with a touchpad remote control.



Portal mode for HbbTV applications

When used in portal mode, HbbTV applications have different requirements. Therefore each application should include a separate 'portal mode' in which it can be launched and used independent of a broadcast. This mode is especially important when:

- the broadcast cannot be accessed for technical reasons;
- when the application is connected via the Red Button mode; in this case the TV picture should be hidden or replaced by a still image;
- note that: navigation commands which are irrelevant in the portal mode should be hidden (i.e. 'Back to the Task bar' and 'Hide Applications');
- navigation links to other applications should launch the applications in the portal mode;
- colour buttons offering functions which are not available should be hidden.

Launching apps

The German ARD network uses the URL parameter to decide whether an HbbTV app is in portal mode or Red-button mode, although in the long term, broadcasters want applications to automatically determine the signal context. The HbbTV standard provides no special features for the inclusion of HbbTV apps in portals.

The providers of portals should have a uniform method of querying whether the app is running in a portal or a signal context.

Return to manufacturer portal

There is no defined return path from HbbTV applications to a portal. Some device manufacturers provide a manufacturer-specific button on the remote control, by which users can access all areas of the manufacturer's portal; with this button, the portal can be controlled from a running HbbTV application. However, generally speaking, the method of return to a portal is the responsibility of the portal manufacturer. The implementation of the function should take place using a button which is not one of the specified application buttons used in the HbbTV standard.





Introduction

These data & privacy guidelines are aimed at developers working within the TV/ broadcast/content distribution domains. They represent a synthesis of current thinking and draw particularly on conditions in the German market. They are based upon current practices and on user studies carried out by the EU-funded Fcontent project.

Background

Television is a key medium of communicating information and a necessary component of independent thought. The right of free access to information is constitutionally protected and is a fundamental condition of a free and democratic society. The collection, analysis and utilization of user behavior and personal data can have an impact on the exercise of this basic human right.

Unlike earlier analogue TV broadcasts, the online connection between the internet and broadcast services creates a feedback channel between viewers and television stations, equipment manufacturers or other third parties. Viewers'

usage of this 'back channel' can be recorded and evaluated.

In May 2014, data protection regulators in private and public-service broadcasters published a common position statement, noting that collection of user data without prior notice to users is legally not allowed. They called for the observance of the principle of 'privacy by default': the basic settings of Smart TVs and web services are defined by manufacturers and providers to take account of the principle of anonymous usage of television.

These guidelines offer practical advice and assistance for you when dealing with living people's personal data (including sensitive personal data).

It's important to protect individuals' data. There can also be criminal and civil sanctions for the content producer when there is an unauthorised disclosure of personal and sensitive data, as well as reputational damage for the production company. Personal data relates to anyone who can be identified from the data or from that and other readily identifiable information e.g. any one or more of their name, address, telephone numbers, personal email addresses, date of birth, bank and pay roll details, next of kin, passport particulars, etc. Sensitive personal data requires extra care and except in limited circumstances can usually only be collected, and used with the express consent of that person. Such information relates to an individual's racial or ethnic orientation, alleged or actual criminal activity and criminal records.

ARD Data Protection position paper

In 2014, the German public service network the ARD set out its position in a Data Protection Position Paper on data protection, with particular focus upon digital broadcasting.

Modern televisions (i.e. Smart TVs) offer access to internet services. It is made possible for viewers to consume additional web content simultaneously with the current TV program (for example, via HbbTV). Equipment manufacturers also offer various internet services for Smart TV devices via their own web platforms. For the viewers, the interlinking of the online world and the TV world is often invisible and seamless.

Unlike earlier analogue broadcasting conditions, the online connection creates a feedback channel, extending from viewers to the television station, the equipment manufacturers or other third parties. The individual usage of this 'back



channel' can be recorded and evaluated.

Television is a key medium of communicating information and a necessary component of independent thought. The right of free access to information is constitutionally protected and is a fundamental condition of a free and democratic society. The collection, analysis and utilization of user behavior would affect the exercising of this basic right.

From a data protection point of view, the following requirements must be observed:

- 1: the anonymous use of Smart TV television services must be ensured. Profiling individual viewing behavior without informed and explicit consent of the audience is inadmissible.
- 2: web and HbbTV services delivered via Smart TV devices are subject to the requirements relevant Teleservices Data Protection Acts. Device manufacturers , broadcasters and all other provider of telemedia must either obtain the appropriate consent of the party/parties concerned or as a minimum observe the following legal requirements:
 - personally identifiable data of the user may only be used provided that this is necessary to provide the services or for accounting purposes; no later than at the beginning of use, users must be fully be informed of the collection and use of their data;
 - only after this step has been taken may providers of telemedia create and analyze user profiles providing that pseudonyms are used and the affected licensees or user concerned has not refused permission;
 - such refusals of permission are to be effectively implemented, and in particular stored characteristics (e.g. cookies) must then be cleared . The right to refuse permission for collection of data must be indicated to users. IP addresses and device IDs are not pseudonyms for the purposes of the Teleservices Data Protection Acts;
 - responsible bodies must ensure that use of profile data is not merged with data which can identify the owner of the pseudonym.
- 3: Compliance with the principle of 'privacy by default'. It is the responsibility of the manufacturer and supplier of Smart TVs and web services to design the

basic settings in such a way that the principle of anonymous use of television is sufficiently taken into account. Communication with web services and the associated two-way communication with device manufacturers, broadcaster or other vendors via the internet is allowed only after full disclosure of the above information and can only be initiated by the users themselves, such as via the use of Red-Button activation in HbbTV. The data stored on the devices data must be subject to the control of the user. In particular, the possibility of management of cookies must be provided to users.

- 4: Smart TVs and HbbTV broadcasts, as well as other web-services, must have safety mechanisms that protect devices and associated traffic from access by unauthorized third parties.

Personal data

Personal Data is data which relates to a living individual who can be identified from that data, or from that data in conjunction with other readily available information, e.g. any one or more of their name, address, images, telephone numbers, personal email addresses, date of birth, bank and pay roll details, next of kin, passport particulars etc. It can also include data such as IP addresses and data automatically collected when using computers and the internet.

Sensitive Personal Data

Sensitive Personal Data is data that relates to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health matters, sexual orientation/life, alleged or actual criminal activity and criminal records. The processing of Sensitive Personal Data requires extra care and, except in limited circumstances, Sensitive Personal Data can usually only be collected and used with the express consent of the person to whom the data relates.

Collection of and access to Personal Data

You and the employees and freelancers working for you will have access to or will routinely acquire Personal Data from many sources and in many forms. For example, Personal Data can be obtained from past, current and future employees, contributors, suppliers and contractors. Personal Data might be contained or provided in letters, correspondence, call logs, programme treatments, run-



ning orders, CVs, CCTV footage, contributor agreements or release forms, contributor application forms, call sheets, criminal record bureau and/or disclosure & barring service checks, medical records, invoices, purchase orders, rushes with captions, bank statements, lists of employees, and employee references.

Personal Data may be in hard copy form e.g. original or copy paper document, photographs and film; or electronic form e.g. PC, laptop, mobile phone, blackberry or memory stick. When proposing to collect Personal Data, care should be taken to limit the data collected to what is actually and likely to be needed. For example, it is unlikely that you would need information regarding a contributor's sexual history, unless it was relevant to the programme.

When you are collecting Personal Data from individuals, tell the individual why you are doing so, who you are and any additional information necessary if specific circumstances require it.

Sharing Personal Data

Data sharing, according to guidance issued by the Information Commissioner's Office includes both the systematic and/or routine sharing of information between and/or within organisations (e.g. pooling data) as well as the exceptional, one-off decisions to share data (e.g. requests from the police). When sharing data, you should ensure that you can demonstrate that the appropriate measures have been taken to protect and appropriately use Personal Data. The first step is to establish that the purpose for the sharing of Personal Data is a valid one and that it is actually necessary to share Personal Data in order to achieve that purpose.

Personal Data for other projects or marketing

You must only use Personal Data for the limited purposes for which it was collected or given to you. For example, it may be that the Personal Data was only provided by a contributor for the purposes of a particular Programme and not for any other use. This means that you must not sell, distribute or provide this Personal Data in any other form to any third party, except where this is necessary to produce and exploit the Programme.

However if you obtain consent from the person to contact them in the future to be involved in other programmes, or to receive marketing information, or to contact employees for opportunities for work etc. then you are permitted to do so. Where you want to provide individuals with electronic marketing messages (e.g. SMS or email marketing), their express consent is required (except in lim-



ited circumstances). This can be agreed when the contributor signs the form or when contracting with an employee or worker.

Privacy notice

A privacy notice is a statement that tells an individual who is collecting information and what it will be used for and details of any third parties the Personal Data is going to be shared with. Privacy notices take a number of forms, for example a notice on a website or a script read out over the telephone. Where you are collecting confidential and/or Sensitive Personal Data, or are intending to use Personal Data in a way that is likely to be unexpected or objectionable to the individual, you must actively communicate your privacy notice i.e. take positive action to provide the privacy notice to the individual, for example, the policy could form part of the contract with the individual.

Third party data handling

If you are using a third party or a sub-contractor who is a Data Processor to handle, process or dispose of Personal Data or confidential information on your behalf you must ensure that they undertake to abide by the relevant data protection terms and conditions.

Where a Data Processor is processing Personal Data that, if lost, may cause harm for a production, it will generally be appropriate to expressly provide in your contact with them that they must comply with these guidelines (as applicable) and include provision in the contract for you to be able to inspect and/or monitor their compliance where practical and necessary.

Use of online tracking tools

The Privacy and Electronic Communications (EC Directive) Regulations 2003 were amended in 2011 to include further requirements in relation to the use of cookies and other information which can be stored on an individual's device. A cookie is a small amount of data, which often includes a unique identifier that is sent to your computer or mobile phone (referred to here as a 'device') browser from a website's computer and is stored on your device's hard drive.

According to the Regulations, cookies or similar devices must not be used unless the subscriber or user of the relevant terminal equipment:

- (a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
- (b) has given his or her consent.



Anonymisation

Anonymisation is the process of rendering data into a form which does not identify individuals and where identification is not likely to take place through its combination with other data. Anonymisation might be used where audience members wish to share their stories or experiences, but the data provided is sensitive. For example, if individuals wanted to contribute to a story about their experiences with a specific organisation, those contributions might need to be aggregated or anonymised in order to provide support for a story without linking it to a specific individual. Anonymisation might also be used where an organisation wishes to share data for research purposes. Data must be anonymized, unless explicit informed consent is given by a user.

Anonymisation might be used where audience members wish to share their stories or experiences, but the data provided is sensitive. For example, if individuals wanted to contribute to a story about their experiences with the NHS, those contributions might need to be aggregated or anonymised in order to provide support for a story without linking it to a specific individual. Anonymisation might also be used where an organisation wishes to share data for research purposes. Effective anonymisation can be used to publish data which would otherwise be personal data. A risk assessment should be carried out before such anonymised data is published to any group sizes.

Launch of applications and inherent communication with manufacturers, broadcasters and other service providers via internet is only allowed after comprehensive information about the information exchange and only initiated by the user his- or herself e.g. pressing the Red Button. Access to web services and the resulting exchange of information with particular manufacturers, broadcasters or internet providers, after comprehensive information about the information exchange, should be initiated by a user his- or herself.

It is the responsibility of the manufacturer and supplier of Smart TVs and web services to design the basic settings so that the principle of anonymous use of television is sufficiently taken into account. Communication with web services and the associated two-way communication with device manufacturers, broadcaster or other vendors via the internet is allowed only after full disclosure of the above information and can only be initiated by the users themselves, such as via the use of Red-Button activation in HbbTV. The data stored on the



devices data must be subject to the control of the user and the possibility of management of cookies must be provided to users.

Data storage management by users

User Data stored on devices must be subject to the control of users. In particular, it must be possible to manage cookies. These requirements have already been implemented by the Association of German public broadcasters the ARD. The ARD is also discussing the possible support of a device configuration set to 'privacy by default' with data protection experts. As a result, any exchange of data, which also takes place when the Red Button functionality is used, should only happen after the approval of a user.

Collecting and accessing personal data

You will have access to or routinely acquire personal data and sensitive personal data in many forms. This information may be from past, current and future employees, contributors, suppliers and contractors.

This information may be in the form of letters, correspondence, call logs, programme treatments, running orders, CVs, CCTV, contributor agreements or release forms, contributor application forms, call sheets, criminal record bureau and/or disclosure & barring service checks, medical records, invoices, purchase orders, rushes with captions, bank statements, list of employees, and employee references. The information can be in hard copy form (original or copy paper document, photographs and film) or in electronic form (PC, laptop, mobile phone or memory stick).

- what should you collect?
- you should only collect what you need, for example it may be reasonable to collect the name and contact details of contributors but it is very unlikely you would need information regarding their sexual history, unless it was relevant to the programme;
- what do you have to tell the person who is giving you the information?
- you should tell the person why you are collecting the information and what you are using it for and how it will be shared, and remind them that they are protected by the DPA;
- how can you use the information?



You can only use personal data for the purposes for which it was collected or given to you. For example, it may be that the personal data was only provided by a contributor for the purposes of a particular Programme and not for any other use. However if you obtain consent from the person to contact them in the future to be involved in other programmes, or to receive marketing information or to contact them for other opportunities, then you are permitted to do so. This can be expressly agreed when the contributor signs the relevant consent form or at the point they provide their information e.g. in an application form.

Data Collection policy

The Data Protection policy of the data collector should be clearly indicated, along with contact details for the responsible person. It should be make clear what kind of data is collected from a user, whether it is anonymous or identifies the user, where and for how long it is stored, and the intended purpose of the collection of the data and the subsequent use of it should be clearly explained. The use of cookies should be indicated if relevant, and details of the duration of their storage and the reason behind their use should be explained.

Each application must show information about data protection and must also offer the option to allow/block cookies. The presentation of data protection information must be consistent and unified, in order that it is recognised across all applications. The user should be required to confirm having read and accepted the data protection conditions only once - the query should not be repeated.

Opt-out

A user's right to refuse consent must be indicated. This consent must be given no later than the beginning of data collection. Refusals of such permission must be effectively implemented and stored data (i.e. cookies) immediately deleted.

Right of user access to data

The right of the user to access details of data collected from him/her should be detailed, along with contact information for the person responsible for Data Protection issues.

Content producer data protection and security

These guidelines set out recommended safeguards that production companies might implement in order to best protect all Personal Data (including Sensitive Personal Data). The guidelines are designed to provide practical advice



to assist in protecting the data of individuals and in turn protecting production companies from civil and/or criminal sanctions and reputational damage as the result of unauthorised disclosure of Personal or Sensitive Personal Data. It is therefore important that all senior staff read these guidelines and that the necessary practical support and guidance is provided for all staff. It is recommended that one senior person within the company takes overall responsibility for data protection policy and practice for the company. Contact details of that senior person should be made available and accessible to all staff.

Policies & personnel

All production companies must have in place an appropriate Data Protection or equivalent Security Policy that sets out how they manage Personal Data within the company and when making programmes. Production companies should ensure that Personal Data is:

- processed fairly and lawfully;
- processed for specified and lawful purposes;
- kept to a minimum when it is collected and processed. Only Personal Data which is adequate, relevant and not excessive should be collected ;
- accurate and, where necessary, kept up-to-date;
- not kept longer than is necessary;
- processed in accordance with the rights of the data subjects under the relevant data protection terms and conditions;
- secured using appropriate technical and organisational measures to protect against unlawful or unauthorised processing of Personal Data and against accidental loss, destruction or damage to Personal Data;
- not transferred outside the European Economic Area unless that country has an adequate level of protection in respect of the processing of Personal Data. Steps should be taken to alert and advise employees and workers of their obligations of your data protection and security policies and practices.

Recommended practices for security of personal data

The production company should regularly review how it stores all Personal Data, including for those individuals whose Personal Data is collected during the course of making the programme, to assess whether the security measures in place can be improved. The less personal data which you have, the more you lessen your risk.



As such, if you have appropriate retention schedules in place which are followed, you lower the risk of data loss. However, there is always a need for some personal data to be held and this should be appropriately secured. Some suggestions for doing so are set out below.

- is any Personal Data or Sensitive Personal Data being stored in a cloud-based storage system or collaboration tool? If so, are there adequate protections in place to ensure the security of data using such storage?
- is unnecessary copying of paper and electronic records for distribution being undertaken? Are staff aware that they should be careful not to leave copies of documents at the photocopier, scanner or fax machine?
- are shredders and/or 'security safe' recycling bins/boxes readily available for disposing of documents and papers potentially containing Personal Data, and are staff reminded to use them properly?
- is the requisite care and attention taken when faxing Personal Data so that only the intended recipient receives the information at the time of sending the information?
- reduce the number of faxes you send, as faxing has been the subject of many civil monetary penalties. If sending a fax is essential, confirming receipt of Personal Data sent via fax is recommended;
- are employees and workers aware that even verbal disclosure of Personal Data can be in breach of the data protection terms and conditions and are they aware of when it is appropriate to disclose?
- if you are selling or disposing of computers, disks or memory sticks, have you taken appropriate steps to ensure that any Personal Data stored on such devices have been securely deleted or made unavailable to future users?

Consideration should be given to the legitimacy of keeping records. For example records of quiz show applicants who are not in the final programme should be destroyed unless they have given permission for the records to be kept for future series or other shows or there is another legitimate business or legal reason to retain them, (e.g. they had an accident at the audition and it is required for health and safety reasons).

Remember: Protect and Respect Personal Data. Don't lose personal data or let it get stolen – treat it as if it were your own personal data.



Resources

General:

FIWARE Media & Content Lab:

<http://lab.mediafi.org>

German public service broadcaster network ARD:

http://www.ard.de/home/ard/ARD_Startseite/21920/index.html

German association of digital media developers:

<http://www.tv-plattform.de>

HbbTV:

HbbTV Open ITV Forum:

<http://www.hbbtv.org/>

Current HbbTV 2.0 standards:

<https://hbbtv.org/resource-library/#specifications>

Developers:

Mozilla Foundation:

https://developer.mozilla.org/en-US/docs/Mozilla/Firefox_OS/TVs_connected_devices/How_to_get_started_with_TV_apps_development

Smart TV Alliance:

<https://developers.smarttv-alliance.org/specification>

Android:

<http://developer.android.com/training/tv/index.html>

Data protection:

<http://ec.europa.eu/justice/data-protection/>



These guidelines have been developed by partners in the Social Connected TV work package of the FICONTENT2 project (2013-2015).

These partners included:

Fraunhofer

Connecting science and industry, Fraunhofer is Europe's leading applied research and development organisation. Fraunhofer FOKUS develops and researches communication systems, applications and IT infrastructures at its headquarters in Berlin; Fraunhofer IAIS performs research and development of technologies, services and solutions for the organisation and indexing of multimedia content.

<https://www.fraunhofer.de/en.html>

Institut für Rundfunktechnik

The Munich-based Institut für Rundfunktechnik is a non-profit broadcast and multimedia technology institute working with numerous clients in the broadcasting, media, communications-engineering, research and higher education sectors. IRT is heavily involved in the technical work of the EBU (the European Broadcasting Union) and is one of the driving forces in the ETSI specification of HbbTV.

<https://www.irt.de/en/home.html>

rbb RUNDFUNK BERLIN-BRANDENBURG

As part of the German ARD (Association of Public Service Broadcasting Corporations), Rundfunk Berlin-Brandenburg is the public broadcaster for Berlin and Brandenburg. RBB broadcasts one TV channel and six radio stations, as well as a range of interactive multimedia services for mobile, teletext and connected TV.

<https://www.rbb-online.de/>



Lancaster University's School of Computing and Communications is an internationally renowned UK-based team of researchers focusing on all aspects of communications and distributed systems, and particularly on support for multimedia and quality of service, the challenges of mobility/ubiquitous computing and problems arising from the increasing levels of heterogeneity in such systems.

<http://www.lancaster.ac.uk/>



Italian consulting and system integrator FINCONS Spa is part of the FINCONS Group, providing tailored and end-to-end software solutions and ICT services to leaders in the fields of media & entertainment, banking & insurance, transportation, utilities & energy, manufacturing and public administration.

<http://www.finconsgroup.com/>

BITTUBES

The Berlin-based BitTubes develops and exploits innovative media and web technologies enabling interactive personalized applications. BitTubes concentrates especially on non-linear video (NLV), an interactive video solution.

<http://www.bittubes.com/>









