



# Politique: Protection

Type: ☒ Original ☐ Addendum  
Responsable: Director of Data  
Équipe responsable: Data  
Date d'entrée en vigueur: 1 November 2022  
Approuvé par: SMT  
Dernière mise à jour:

S'applique à :

- ☐ Niveau global ☐ Tout bureau sauf global  
☒ Tout bureau ☐ Autres, spécifiez

---

Version 1.2

---

Dernière révision par: Paul Uithol, Jessie Pechmann

---

Prochaine date de révision: June 2024

Historique des versions:

Final draft	3 June 2022	Final draft proposed for adoption by SMT
1.0	1 November 2022	First approved version
1.1	1 June 2023	Address comments from external review
1.2	1 October 2023	Clarity of review and approval process.

Contents:

<b>1. Purpose</b>	<b>3</b>
<b>2. Application and Practical Implementation</b>	<b>4</b>
<b>3. Definition and Scope</b>	<b>5</b>
<b>4. Required Steps Before Starting Open Mapping Projects</b>	<b>7</b>
<b>5. Revisions and versioning</b>	<b>9</b>
<b>6. Roles and responsibilities</b>	<b>11</b>
<b>7. Policy implementation</b>	<b>12</b>
<b>Annex 1: Resources, training, and monitoring</b>	<b>13</b>

# 1. Purpose

## 1. Objectif

***Les données spatiales et les activités de cartographie sont susceptibles de créer des risques ou de porter préjudice aux personnes et aux communautés. HOT, en tant qu'agence menant et soutenant des activités de cartographie et produisant des données spatiales ouvertes et librement disponibles avec peu de contraintes sur leur usage; est responsable de la compréhension, de l'évaluation, de l'atténuation et de la protection contre les risques et les préjudices découlant des activités qu'elle entreprend ou qu'elle soutient.***

Cette politique définit la manière dont les intervenants dans les activités de collecte, de stockage et d'utilisation des données peuvent s'acquitter de ces responsabilités, et représente l'engagement de HOT en faveur de pratiques responsables et éthiques visant à protéger les personnes contre les préjudices. Les parties prenantes comprennent le personnel de HOT, les sous-traitants et les volontaires déployés, ainsi que les communautés (OSM) qui participent aux activités de collecte de données financées par HOT ou d'autres donateurs.

L'approche de HOT en matière de données éthiques s'appuie sur les principes de données "ouvertes et accessibles", "données utiles et utilisables", "inclusives et représentatives" et "données et protection éthiques". Plus précisément, "Données et protection éthiques" signifie que le HOT vise la collaboration la plus significative en matière de gestion et de planification des données avec les personnes et les communautés avec lesquelles nous travaillons, et qu'il respecte les politiques et les orientations visant à minimiser les risques de préjudice, y compris les évaluations d'impact et le consentement éclairé pour toute collecte ou utilisation de données. Cela comprend les quatre principes suivants :

1. Appliquer un processus pratique d'engagement et de consentement éclairé dans l'ensemble de nos activités, y compris pour la télédétection et la numérisation (tout en tenant compte d'un environnement technologique de plus en plus sophistiqué).
2. Veiller au respect des croyances, des cultures, des modes de vie et des choix des communautés dans la prise de décision concernant la collecte et le partage des données, ainsi que dans l'utilisation des informations collectées. Impliquer les partenaires dans le processus d'utilisation éthique de l'information.
3. Réaliser des évaluations des risques et des impacts des données afin d'évaluer et de minimiser les risques de préjudice pour tous les projets, en collaboration avec les communautés concernées. Dans les situations où le conflit est un facteur, suivre la "politique de cartographie des zones de conflit".

4. Veiller à ce que tous les employés de HOT respectent l'application des principes de protection des données.

Consultez la politique : [☰ Policy: HOT activities & mapping in conflict zones](#) pour plus d'informations sur la cartographie dans les zones de conflit.

## 2. Application et mise en œuvre

L'outil d'éthique et de protection des données est le principal instrument de mise en œuvre de cette politique. Tous les projets de cartographie sur le terrain, les activations et les projets de cartographie à distance dans les zones de conflit/à haut risque soutenus par HOT ou utilisant l'infrastructure HOT doivent remplir cet outil avant de commencer leurs activités (les projets de cartographie à distance dans les zones pacifiques et stables n'ont pas besoin de remplir cet outil).

Ce document n'a pas pour but de créer des obstacles au travail normal ou d'alourdir la bureaucratie. Pour la plupart des projets HOT (dans des contextes pacifiques, ne traitant pas de données sensibles), l'exercice devrait prendre moins d'une heure.

Tous les cadres supérieurs et les directeurs de HOT doivent connaître ce document et être conscients des circonstances dans lesquelles les activités, les projets et les données doivent être évalués en fonction de leur dangerosité potentielle. Les chefs de projet travaillant dans des contextes à risque, tels que les zones de conflit, doivent également le connaître.

Le présent document, ainsi que les orientations et les outils qui le complète, doivent pouvoir être consultés et mis à la disposition de toute personne concernée par le risque de protection au sein de l'organisation. En outre, dans tous les cas où un risque de protection est susceptible de survenir (comme la cartographie dans les zones de conflit), le(s) directeur(s) responsable(s) des projets (normalement les directeurs de hub, mais dans le cas de projets gérés par des membres de l'équipe mondiale, le responsable principal ou le directeur dans la ligne hiérarchique) est (sont) chargé(s) de veiller à ce que cette politique soit consultée, suivie, signée et conservée avec d'autres documents relatifs au projet.

### 3. Définition et objet

Le mot "protection" est utilisé ici d'une manière similaire à son usage courant dans le domaine humanitaire, qui englobe deux définitions de base :

1. Protéger la vie, les moyens de subsistance, la sécurité, la santé et la dignité des personnes touchées, et
2. Veiller à ce que nos propres actions n'entraînent pas ou ne perpétuent pas la discrimination, les abus, la négligence ou la violence.

Dans les situations humanitaires ou de conflit, les deux définitions s'appliquent. Toutefois, dans les contextes de développement pacifique et stable (par opposition aux contextes humanitaires ou de conflit), l'accent est mis sur la définition 2, qui peut être résumée par l'injonction commune "Ne pas nuire".<sup>1</sup>

Dans le cadre de l'étude :

- Risque de préjudice pour les personnes et les communautés qui sont cartographiées ou au sujet desquelles des données sont collectées (par opposition au personnel et aux cartographes) pendant la collecte des données et les activités de cartographie, ou résultant de l'utilisation et de l'analyse de ces données. Ceci couvre :
  - les activités propres à HOT
  - les projets directement soutenus par HOT (financement, soutien matériel ou en nature) ou utilisant l'infrastructure de HOT (Tasking Manager ou similaire),
  - toutes les données mises à disposition via des plateformes de données ouvertes telles que OpenStreetMap,
  - toutes les données que HOT possède ou gère (données ouvertes ou non) et dont une évaluation dûment diligente montrerait qu'elles créent un risque et/ou un préjudice pour les personnes ou les communautés,
  - et enfin les données détenues et gérées par d'autres qui sont directement issues des activités soutenues par HOT.

#### **Hors champ :**


- Sûreté et sécurité des opérations. Ce document se concentre sur l'impact potentiel et le risque pour les communautés cartographiées suite à la création de données spatiales ouvertes, et non sur la sûreté et la sécurité des cartographes. La sûreté et la sécurité

---

<sup>1</sup> Du latin *Primum non nocere*, un principe du travail humanitaire et du développement emprunté au domaine de la santé, qui, selon l'article du lien ci-dessus, est "invoqué lorsque l'on débat de l'utilisation d'une intervention qui comporte un risque évident de dommage, mais une chance moins certaine de bénéfice".

Parfois, cette maxime est élargie à "Ne pas nuire davantage" - reconnaissant que le travail humanitaire est plus ou moins par définition dans des contextes où le mal est déjà répandu, et l'impératif est de minimiser le risque de dommage supplémentaire de nos interventions, en équilibre avec leurs avantages.

sont importantes et se recoupent quelque peu avec les aspects de protection, mais qui est ultimement une préoccupation distincte. Ceci est expliqué dans le document

 HOT Policy: Security .

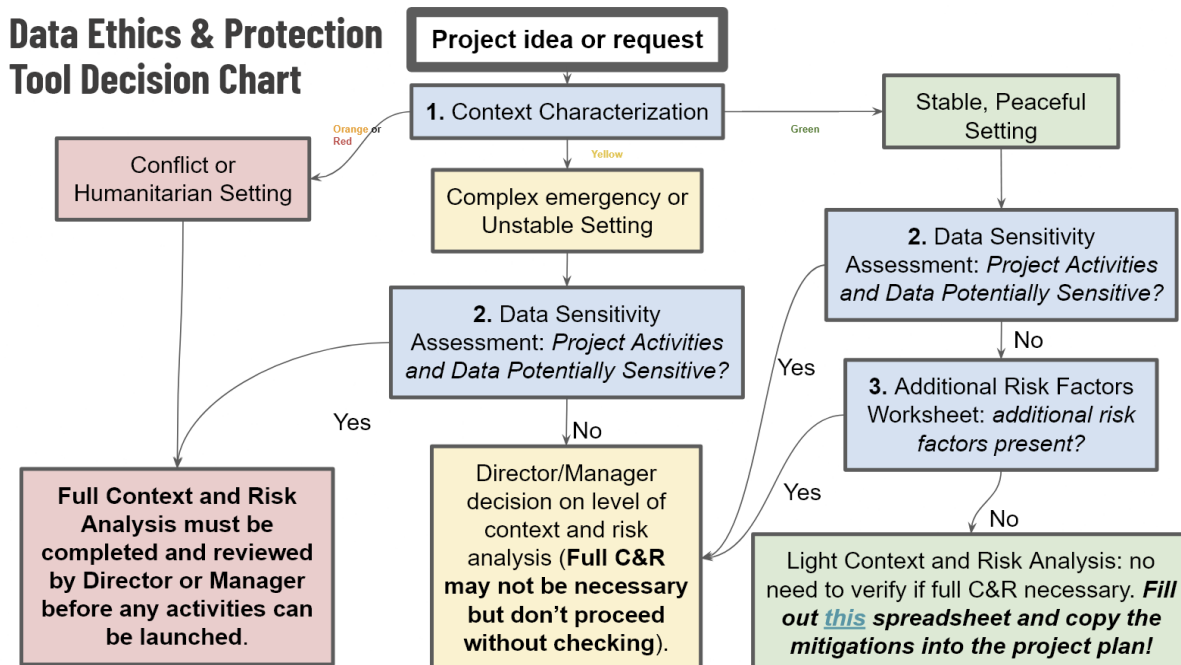
- Les données stockées sur des systèmes privés, fermés et/ou propriétaires exploités ou contrôlés par HOT. Bien que la protection implique la responsabilité d'examiner attentivement quelles données devraient être recueillies et stockées, la détermination des mesures à prendre pour sécuriser adéquatement les données sensibles qui en résultent (parfois appelée protection des données) sera traitée dans le cadre de la politique sur la sécurité de l'information.
- L'utilisation par d'autres de logiciels libres et open source (FOSS) créés ou soutenus par HOT et qui échappent au contrôle et à l'infrastructure de HOT. Les licences de ces logiciels sont claires : toute personne est libre d'utiliser le logiciel et HOT n'est pas responsable de sa conduite.
- Utilisation par d'autres de données ouvertes fournies ou soutenues par HOT. L'utilisation des données OpenStreetMap est régie par la Open Database License, qui autorise toute utilisation à condition que les données soient attribuées, partagées et maintenues ouvertes. HOT (ou tout autre créateur de ces données ouvertes) n'est pas responsable de la conduite des utilisateurs.

Il convient de noter qu'aucune de ces mesures ne rejette la responsabilité de la création de données ouvertes susceptibles de causer des dommages. D'une certaine manière, une fois diffusées dans le monde, les données ouvertes ne peuvent être rappelées. Par conséquent, leur création et leur diffusion impliquent des responsabilités.

## 4. Étapes nécessaires avant de lancer des projets de cartographie ouverte

- Tous les projets de cartographie ouverte soutenus par HOT et **comportant une dimension de terrain** doivent faire l'objet d'une évaluation des risques en matière de protection.
- Toutes les "**activations**" doivent faire l'objet d'une évaluation des risques de protection dans le cadre du "size-up".
- Certains projets de cartographie à distance basés sur le gestionnaire de tâches (principalement ceux qui se situent dans des zones à haut risque et/ou très sensibles) nécessitent une évaluation du risque de protection.

Dans de nombreux cas, l'évaluation du risque de protection peut être un processus très léger ; cette politique n'a pas pour but d'entraver ou de gêner les activités habituelles d'Open Mapping. Au contraire, elle peut encourager un dialogue constructif sur l'utilisation potentielle des données et ses implications avec les communautés concernées. L'outil d'éthique et de protection des données contient un organigramme montrant l'arbre de décision depuis une idée ou une demande de projet jusqu'au niveau de supervision requis pour l'évaluation des risques de protection :



Il existe trois catégories de projets, correspondant aux cellules du bas de l'organigramme. Dans tous les cas, l'[outil d'éthique et de protection des données](#) doit être rempli. La différence entre les niveaux de risque vert, jaune et rouge est le niveau de supervision requis :

- **Vert**: Une analyse légère du contexte et des risques est requise. Cela signifie qu'un projet se situe (a) dans un environnement stable et paisible, (b) n'implique pas de données sensibles, et (c) ne présente pas de facteurs de risque supplémentaires. Le responsable du projet (qui peut être un bénéficiaire d'une subvention communautaire ou un mentor) effectue un simple exercice sur une feuille de calcul. L'exercice devrait durer une heure.
- **Jaune**: Moyen ou incertain. Décision du directeur ou du gestionnaire sur le niveau d'évaluation requis.
- **Rouge**: Équivalent à une zone de conflit et/ou à la collecte de données très sensibles ; nécessite automatiquement une supervision au niveau du directeur (ou au niveau du cadre supérieur si délégué) du processus d'évaluation des risques avant le début des activités.

Pour les projets des catégories jaune ou rouge, l'ensemble du processus doit être complété et approuvé par le directeur qui supervise directement le projet. Avant de commencer l'évaluation des risques proprement dite, ajoutez les données pertinentes pour l'évaluation et les examens dans l'onglet "0. Proposition et portée". Chaque évaluation des risques se compose de 5 étapes, qui sont expliquées plus en détail dans l'outil :

1. **Catégorisation du contexte** : identifier le type de contexte. Il en résulte une étiquette de contexte rouge, orange, jaune ou verte.
2. **Évaluation de la sensibilité des données** : toutes les données n'ont pas le même potentiel de nuisance, et celui-ci varie en fonction des facteurs contextuels. Identifier toutes les données potentiellement sensibles dans le contexte identifié.
3. **Facteurs de risque additionnels** : un lieu donné peut être généralement paisible et stable, mais peut nécessiter plus qu'une évaluation légère des risques de protection si des facteurs contextuels spécifiques sont présents, tels que des épidémies ou des élections.
4. **Évaluation des risques de protection** : identifier les risques spécifiques en évaluant la vulnérabilité, la probabilité et l'impact. Élaborer des mesures d'atténuation et modifier le projet en fonction des risques identifiés.
5. : examinez l'outil de protection et d'éthique des données dûment rempli. Examinez si le niveau de risque est acceptable ou si des modifications et des mesures d'atténuation supplémentaires sont nécessaires. Si le risque résiduel est jugé inacceptable, *la conséquence ultime peut être que le projet ne doit pas être poursuivi sous la forme proposée*. Il existe deux niveaux d'approbation :
  - a. **Révision** : en fonction de la confiance accordée à l'évaluation par le personnel chargé de l'évaluation des risques, demandez à une ou deux personnes des



points focaux de protection ou à une personne connaissant bien le contexte de réviser l'évaluation complète et de formuler des commentaires et des suggestions. Si l'évaluation est satisfaisante, les réviseurs doivent apposer leur signature.

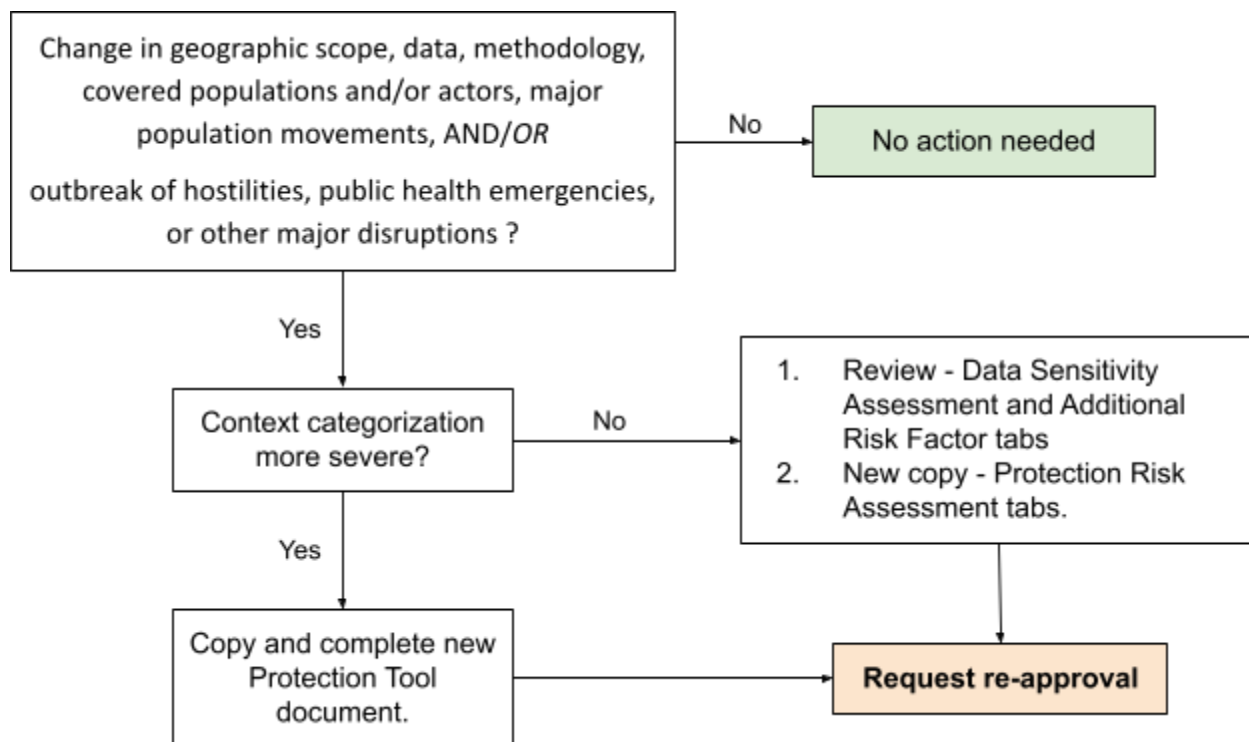
- b. **Approbation** : en principe, l'approbation finale doit être donnée par le directeur qui supervise directement le membre du personnel chargé de réaliser l'évaluation des risques de protection, qui doit être un membre de l'équipe chargée de mettre en œuvre et d'exécuter les activités proposées. L'approbation de l'évaluation doit se situer dans la même hiérarchie que la mise en œuvre et l'exécution du projet afin de garantir un contrôle significatif des mesures d'atténuation proposées et d'exiger une réévaluation si nécessaire. Dans des circonstances exceptionnelles et en étroite coordination, cette autorité peut être déléguée à un autre directeur ou à un membre de l'équipe de direction. Pour l'approbation finale:
- i. Examiner l'évaluation des risques pour y déceler d'éventuelles lacunes.
  - ii. Examiner les mesures d'atténuation pour s'assurer de la clarté de la mise en œuvre sur la base de la faisabilité, de la capacité, de l'appropriation claire et de l'efficacité.
  - iii. S'assurer de la compréhension de tous les risques et de toutes les mesures d'atténuation afin d'orienter les travaux futurs et de répondre
  - iv. aux questions éventuelles concernant le projet.

La feuille de calcul "Outil de protection et d'éthique des données" complétée doit être conservée avec la documentation pertinente du projet dans le dossier du projet.

## 5. Révisions et versions

Au fil du temps, des changements dans la portée du projet, la zone d'opérations, les demandes des partenaires ou les circonstances locales peuvent signifier que l'évaluation de l'éthique et de la protection des données devient inadéquate et doit être révisée. Une évaluation doit être révisée dans les cas suivants :

- En cas de changements significatifs dans la portée du projet, tels que la zone d'opérations couverte par la collecte de données et la cartographie, les types de données collectées ou la méthodologie.
- Demande de cartographie émanant de partenaires supplémentaires qui élargissent les acteurs couverts, les populations touchées ou les données demandées.
- Mouvements de population à une échelle suffisamment grande pour affecter la dynamique et les risques de la communauté.
- Déclenchement d'hostilités, urgences de santé publique ou autres perturbations majeures.



Si l'une de ces situations se produit, réévaluez la première étape : "1. catégorisation du contexte". Si aucune de ces situations ne se produit, il est toujours recommandé de réévaluer périodiquement la catégorisation du contexte, au moins une fois par semestre. Sur la base de la réévaluation, procédez comme suit :

1. Si le résultat de l'arbre de décision de la catégorisation du contexte est inchangé (toujours rouge/jaune/vert) ou si sa gravité a diminué, l'évaluation actuelle peut être modifiée comme suit :
  - a. Examinez les onglets "2. Évaluation de la sensibilité des données" et "3. Facteurs de risque supplémentaires", et mettez-les à jour si nécessaire.
  - b. Pour préserver les risques et les mesures d'atténuation précédents, renommez la version actuelle de l'onglet "4. Évaluation du risque de protection" en fonction de la date de son approbation initiale - par exemple, "4. Évaluation du risque de protection\_11 mars 2023"
  - c. Créez une nouvelle copie de l'onglet "4. Évaluation du risque de protection" dans l'outil actuel, et modifiez-le en y ajoutant la date de la nouvelle évaluation - par exemple, "4. Évaluation du risque de protection\_20 juin 2023\_dernier". Complétez la nouvelle évaluation des risques.
  - d. Demander l'approbation de l'évaluation et l'indiquer explicitement avec une nouvelle série de signatures dans l'onglet "CHECKLIST and Approvals" (liste de contrôle et approbations).
2. Si le résultat de l'arbre de décision de la catégorisation du contexte a augmenté en gravité - passant du vert au jaune, ou du jaune au rouge - une nouvelle évaluation complète doit être créée.
  - a. Datez l'ancien document - par exemple, "Outil d'éthique et de protection des données\_réponse à la sécheresse en Somalie\_11-03-2023".
  - b. Créez une nouvelle copie de l'outil d'éthique et de protection des données et répétez le processus décrit au point 4. Étapes à suivre avant de lancer un projet de cartographie ouverte. Datez et versionnez le nouveau document - par exemple, "Outil d'éthique et de protection des données\_réponse à la sécheresse en Somalie\_20-06-2023\_dernier"
  - c. Demandez l'examen et l'approbation de l'évaluation mise à jour.

## 6. Roles and responsibilities

Rôle	Tâches	Responsabilité
Gestionnaire de projet	Compléter l'outil d'éthique et de protection des données sous la supervision du gestionnaire principal ou du directeur, et en collaboration avec l'équipe du projet - en consultation avec les communautés (potentiellement) affectées si possible.	<ul style="list-style-type: none"> <li>• Compléter l'outil et l'évaluation des risques</li> <li>• Identification des risques</li> <li>• Recherche d'informations et consultation adéquates</li> <li>• Fournir une représentation honnête, juste et précise</li> <li>• Demande d'examen et d'approbation en temps utile</li> </ul>
Supervision directe des chefs de projet (souvent des chefs d'équipe)	Veiller à ce que l'outil de protection et d'éthique des données soit correctement rempli et que les risques éventuels soient signalés, atténués et intégrés dans la mise en œuvre et l'exécution du projet.	<ul style="list-style-type: none"> <li>• Superviser la planification et la mise en œuvre des projets</li> </ul>
Réviseur	<p>Examiner les évaluations terminées sur la base de l'expérience et de la connaissance du processus d'évaluation des risques, des facteurs contextuels et/ou des situations de conflit.</p> <p>Une liste régulière de révisions sera sélectionnée et communiquée.</p>	<ul style="list-style-type: none"> <li>• Revue des évaluations achevées</li> </ul>
Membres de l'équipe de direction (SMT)	Superviser et soutenir la mise en œuvre et l'exécution des projets de manière responsable et en assumer la responsabilité finale.	<ul style="list-style-type: none"> <li>• Signer et approuver les évaluations complétées et révisées</li> <li>• Supervision de</li> </ul>

		l'application et de la mise en œuvre
Conseil d'administration	Cette politique est placée sous la supervision du comité "Gestion des risques" du Conseil d'administration.	<ul style="list-style-type: none"> <li>Assurer l'intégration des risques prévalents dans le registre des risques</li> </ul>